

LA SEGURIDAD CIBERNÉTICA

# MARÍTIMA EN EL HEMISFERIO OCCIDENTAL

Introducción y Directrices



**OEA**

Más derechos  
para más gente

LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices



LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA** **EN EL HEMISFERIO** **OCCIDENTAL**

---

Introducción y Directrices



**OEA**

Más derechos  
para más gente

## DERECHOS DE AUTOR (2021) Organización de los Estados Americanos

Todos los derechos reservados. Ninguna porción de esta publicación podrá reproducirse o transmitirse de ninguna forma o por cualquier medio, total o parcialmente, sin el consentimiento expreso de la Secretaría General de la Organización de los Estados Americanos.

Elaborado y publicado por el Programa de Protección Marítima y Portuaria del Comité Interamericano contra el Terrorismo (CICTE).

Los contenidos de esta publicación se presentan exclusivamente con fines informativos y no representan la posición oficial de la Organización de los Estados Americanos, su Secretaría General o sus Estados Miembros.

Esta publicación ha sido posible gracias al apoyo financiero del Gobierno de Canadá.

Agradecemos su interés en esta guía. Sus comentarios sobre cómo usted ha utilizado esta guía y si le ha ayudado a mejorar la respuesta a incidentes de ciberseguridad marítima serán información valiosa que podremos utilizar para ayudar a diseñar proyectos futuros.

Por favor comuníquese con el Programa de Protección Marítima y Portuaria de CICTE al correo electrónico [CICTE@oas.org](mailto:CICTE@oas.org) para compartir sus comentarios.

## OAS Cataloging-in-Publication Data

La seguridad cibernética marítima en el Hemisferio Occidental : introducción y directrices / [Elaborado y publicado por el Programa de Protección Marítima y Portuaria del Comité Interamericano contra el Terrorismo (CICTE)].

v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.17)

ISBN 978-0-8270-7241-1

1. Computer security. 2. Security, International. 3. Transportation--Security measures. 4. Cyberterrorism. 5. Shipping--Security measures. 6. Harbors--Security measures. I. Inter-American Committee against Terrorism. II. OAS/CICTE Maritime and Port Security Program. III. Organization of American States. Secretariat for Multidimensional Security. IV. Series. OEA/Ser.D/XXV.17



# CRÉDITOS

## Luis Almagro

Secretario General

Organización de Estados Americanos (OEA)

## Arthur Weintraub

Secretario de Seguridad Multidimensional

Organización de los Estados Americanos (OEA)

## Alison August Treppel

Secretaria Ejecutiva

Comité Interamericano contra el Terrorismo  
Organización de los Estados Americanos (OEA)

## Violanda Botet

Secretaria Ejecutiva

Comité Interamericano contra el Terrorismo  
Organización de los Estados Americanos (OEA)

## Equipo Técnico de la OEA

### Programa de Protección Marítima y Portuaria

Lisbeth Laurie

Ricardo Desgarenes

### Programa de Ciberseguridad

Kerry-Ann Barrett

Diego Subero

Sofia Hunter

## Interna

Karen Grubb

## Colaboradores

Hudson Trident

Max Bobys

Andrew Baskin

## Diseño Gráfico

María Paula Lozano



# ÍNDICE

<b>Resumen ejecutivo</b>	<b>09</b>
<b>Lista de acrónimos</b>	<b>11</b>
<b>1.0 - Introducción</b>	<b>13</b>
<b>2.0 - El riesgo cibernético en el ámbito marítimo</b>	<b>15</b>
<b>2.1 - Por qué la seguridad cibernética es importante para los puertos del hemisferio occidental</b>	<b>15</b>
<b>2.1.1</b> - Digitalización y automatización de las operaciones portuarias y marítimas	17
<b>2.1.2</b> - Las organizaciones marítimas como centros y depósitos de datos logísticos	17
<b>2.2 - De qué manera son vulnerables los puertos y los buques</b>	<b>18</b>
<b>2.2.1</b> - Condiciones operativas	18
<b>2.2.2</b> - Vulnerabilidades humanas	19
<b>2.2.3</b> - Interconexión entre puertos y buques	20
<b>2.2.4</b> - Intersección ciberfísica	21
<b>2.3 - Amenazas de seguridad cibernética</b>	<b>22</b>
<b>2.3.1</b> - Tipos de actores de las amenazas cibernéticas	22
<b>2.3.2</b> - Estudios de casos	23

## 3.0 - Reglamentos y directrices ----- 25

### 3.1 - Intentos internacionales para abordar las cuestiones de la seguridad cibernética marítima ----- 26

3.1.1 - La OMI y el transporte marítima ----- 26

3.1.2 - La OMI y los puertos ----- 27

### 3.2 - Legislaciones y normativas nacionales -----28

3.2.1 - Estrategias nacionales de seguridad cibernética ----- 28

3.2.2 - Legislación nacional y supranacional y normativa multilateral --- 28

### 3.3 - Marcos políticos y normas industriales útiles ----- 30

3.3.1 - Marco de Seguridad Cibernética del Instituto de Nacional de Estándares y Tecnologías de Estados Unidos ----- 30

3.3.2 - Normas 27000 y 28000 de la Organización Internacional de Normalización ----- 32

3.3.3 - Controles del Centro de Seguridad de la Información ----- 32

### 3.4 - Directrices del sector ----- 33

3.4.1 - Seguridad cibernética portuaria: Buenas prácticas de la Agencia Europea de Seguridad de las Redes y de la Información para la seguridad cibernética en el sector marítimo ----- 33

3.4.2. - Guía de buenas prácticas del Reino Unido ----- 33

### 3.5 - Requisitos de privacidad de los datos ----- 34

## 4.0 - Pasos iniciales para desarrollar las capacidades de seguridad cibernética de una organización ----- 35

### 4.1 - Establecimiento de supervisión ----- 37

### 4.2 - Definición de las partes interesadas ----- 37

### 4.3 - Creación de un comité directivo de seguridad cibernética ----- 38

4.3.1 -Estrategias para impulsar el cambio ----- 39



4.4 -	<b>Evaluación preliminar de la capacidad de toda la organización</b>	-	<b>40</b>
4.5 -	<b>Estrategia de seguridad cibernética y plan de implementación</b>	--	<b>41</b>
4.5.1 -	Estrategia de seguridad cibernética	-----	41
4.5.2 -	Plan de seguridad cibernética	-----	42

## 5.0 - **Mejores prácticas** ----- **43**

5.1 -	<b>Mejores prácticas de gobernanza y política</b>	-----	<b>44</b>
5.1.1 -	Seguridad de los datos	-----	44
5.1.2 -	Políticas sobre tecnología	-----	45
5.2 -	<b>Mejores prácticas operativas</b>	-----	<b>47</b>
5.2.1 -	Capacitación	-----	47
5.2.2 -	Manejo del control de acceso ciberfísico	-----	49
5.2.3 -	Seguridad del correo electrónico	-----	50
5.2.4 -	Protección contra la ingeniería social	-----	51
5.2.5 -	Control de acceso	-----	52
5.2.6 -	Recopilación y análisis de información sobre amenazas cibernéticas	-----	54
5.2.7 -	Intercambio de información	-----	54
5.2.8 -	Seguridad de la red, gestión de la vulnerabilidad y conocimiento de situaciones	-----	55
5.2.9 -	Gestión de la cadena de suministro y de terceros	-----	57
5.3 -	<b>Preparar una respuesta a incidentes cibernéticos</b>	-----	<b>58</b>
5.3.1 -	Crear un plan de respuesta a incidentes	-----	58
5.3.2 -	Planear la continuidad de las operaciones y la recuperación posteriores a un desastre	-----	60
5.3.3 -	Desarrollar relaciones con los terceros que ayudarán en la respuesta y recuperación de incidentes	-----	61
5.3.4 -	Realizar simulacros y prácticas de respuesta a incidentes cibernéticos	-----	62

## 6.0 - **Conclusión** ----- **63**

## **References** ----- **64**





# RESUMEN EJECUTIVO

El aumento de la digitalización y la automatización en el ámbito marítimo<sup>1</sup> ha traído consigo mejoras en la eficiencia y la competitividad, pero también en el riesgo cibernético general del sector. En el hemisferio occidental, el sector marítimo es crucial para el flujo del comercio, y la protección de las operaciones y los datos que sustentan esas operaciones guarda una importancia creciente para las economías nacionales y regionales.

La Organización de los Estados Americanos (OEA), un organismo internacional, a través del Comité Interamericano contra el Terrorismo (CICTE), ha elaborado este documento general con el fin de:

- 1.** Ayudar a las partes interesadas del hemisferio occidental a comprender los riesgos cibernéticos en el sector marítimo.
- 2.** Ofrecer un breve resumen de las principales reglas y normas internacionales que están desarrollando actualmente los organismos internacionales y los Estados para hacer frente a estos riesgos.
- 3.** Establecer las medidas iniciales que pueden adoptar las organizaciones marítimas para gestionar el riesgo cibernético.
- 4.** Destacar algunas de las mejores prácticas que deben tener en cuenta las organizaciones marítimas en la implementación de sus programas de gestión de los riesgos cibernéticos.

### **Las consideraciones de alto nivel incluyen:**

- Las organizaciones marítimas son blanco de ataques cibernéticos por muchas razones, como su creciente complejidad informática y operativa y su papel como centros de datos de compañías navieras, de transporte por carretera, de logística y de almacenamiento fuera del muelle.
- Diversos actores marítimos del hemisferio occidental, como los puertos, los transportistas y los proveedores de logística, han sido víctimas de importantes y costosos ataques cibernéticos.
- Las normas internacionales sobre la forma de gestionar los riesgos de seguridad cibernética

marítima están evolucionando, pero van a la zaga de las necesidades operativas. Las directrices y estándares no vinculantes pueden ayudar a las organizaciones marítimas a elaborar sus propios programas eficaces de gestión de riesgos cibernéticos y de seguridad cibernética.

- Las mejores prácticas para mejorar la gestión del riesgo cibernético y la seguridad cibernética ya existen y se describen en este documento con el fin de ayudar a las entidades de la región a llevar a cabo una evaluación inicial de su capacidad de seguridad cibernética de base para medir las capacidades de seguridad cibernética con que cuentan.
- Un mayor conocimiento de las normas internacionales y de las mejores prácticas para gestionar el riesgo de seguridad cibernética en el ámbito marítimo puede ser de especial utilidad para los Estados miembros de la OEA, algunos de los cuales se encuentran en las primeras fases de estudio e implementación de programas de digitalización marítima.
- Los países del hemisferio occidental, especialmente los de América Latina, están desarrollando rápidamente planes nacionales de seguridad cibernética y aumentando las formas de compartir información y dar respuesta pronta a los incidentes de seguridad cibernética. Los programas de seguridad marítima y cibernética del CICTE están ayudando a los Estados en estos esfuerzos y esta publicación forma parte de una serie de informes que abordan diversos aspectos del ciberespacio en la región.





# LISTA DE ACRÓNIMOS

<b>CERT</b>	Equipos comunitarios de respuesta a emergencias
<b>CICTE</b>	Comité Interamericano contra el Terrorismo
<b>ERP</b>	Planificación de recursos empresariales
<b>ISO</b>	Organización Internacional de Normalización
<b>PBIP</b>	Código internacional para la protección de los buques y de las instalaciones portuarias
<b>MTS-ISAC</b>	Centro de análisis e intercambio de información sobre sistemas de transporte marítimo
<b>NIST CSF</b>	Marco de Seguridad cibernética del Instituto de Nacional de Estándares y Tecnología
<b>OEA</b>	Organización de los Estados Americanos
<b>OMI</b>	Organización Marítima Internacional
<b>RFID</b>	Identificación por radiofrecuencia
<b>SCADA</b>	Control de supervisión y adquisición de datos
<b>SMS</b>	Servicio de mensajes cortos
<b>SOLAS</b>	Seguridad de la Vida Humana en el Mar
<b>SPF</b>	Convenio de Remitentes
<b>TLP</b>	Protocolo de semáforos
<b>UE</b>	Unión Europea
<b>USCG</b>	Guarda Costera de Estados Unidos

LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices





# 1.0

## INTRODUCCIÓN

El transporte marítimo es fundamental para el movimiento de mercancías que sustentan la economía mundial. La infraestructura marítima facilita el flujo de bienes esenciales, como alimentos, medicamentos y energía. Como parte de la columna vertebral del comercio y la economía mundial, el sector marítimo está digitalizando, y en algunos casos automatizando, cada vez más sus operaciones, y los llamamientos para que el sector acelere este proceso se han multiplicado<sup>2</sup>. Dado que la cadena de suministro “justo a tiempo” se basa en las eficiencias que brinda la digitalización, este proceso se traducirá en un aumento de la eficiencia y en una industria más receptiva a las necesidades de una economía mundial en evolución.

Como se ha visto en otras industrias, el cambio hacia un entorno más digitalizado, como el comercio electrónico y el intercambio de datos, conlleva el correspondiente incremento del riesgo cibernético. Las operaciones y los datos marítimos son vulnerables a las amenazas cibernéticas. Los países del hemisferio occidental son cada vez más conscientes de ello y, en respuesta, están expresando sus preocupaciones políticamente a nivel regional. En la práctica, también están elaborando planes de seguridad cibernética a nivel nacional para hacer frente a estos riesgos a nivel operativo<sup>3</sup>. Sin embargo, aún queda trabajo por hacer para desarrollar y adaptar esos planes nacionales para hacer frente a las crecientes preocupaciones en materia de seguridad cibernética en el sector marítimo.



Las amenazas cibernéticas afectan a todos los sectores industriales, y en el hemisferio occidental se ha prestado mucha atención a aumentar la seguridad de los sistemas financieros y bancarios y de los servicios gubernamentales. La necesidad de promover la seguridad cibernética en el ámbito marítimo es de igual importancia, ya que la infraestructura marítima presenta su propio conjunto de riesgos y vulnerabilidades. Por ejemplo, el sector marítimo depende en gran medida de sistemas como las complejas tecnologías de la información y las tecnologías operativas y también está sujeto cada vez más al uso de dispositivos habilitados para el Internet de las cosas y de sistemas automatizados que integran las comunicaciones, el control y el procesamiento de la información. Las amenazas cibernéticas a esta infraestructura digital pueden generar interrupciones operativas y corrupción de datos en la industria marítima, lo que puede tener graves efectos para el comercio, la economía y la seguridad. En consecuencia, los dirigentes de las organizaciones marítimas deben conocer el panorama de los riesgos cibernéticos marítimos y tomar medidas para mitigarlos, tanto internamente como para el sector marítimo en su conjunto.

Este documento está destinado a los ejecutivos, altos directivos y otros responsables de la infraestructura marítima terrestre o de las instalaciones relacionadas que participan en la logística de las cargas marítimas y personas del sector en el hemisferio occidental, entre ellos:

- Los altos ejecutivos, como los directores ejecutivos y generales.
- Los encargados de la gobernanza y la supervisión, como las juntas de comisionados o los directorios.
- Los directores técnicos sin responsabilidades en materia de tecnología de la información, como los de operaciones de las terminales.
- Los directores administrativos, como los de finanzas, jurídicos y de recursos humanos.

Este documento informa a los líderes de la industria marítima sobre los requisitos, las directrices y las mejores prácticas que sus organizaciones pueden utilizar e incorporar para gestionar el riesgo cibernético, impulsar la madurez de la capacidad de seguridad cibernética de la organización y fortalecer la resiliencia operativa. Este documento también identifica y analiza estudios de casos específicos del sector marítimo, incluidos algunos en el hemisferio occidental, que ilustran los principales problemas de seguridad cibernética y de gestión de los riesgos cibernéticos a los que se enfrentan las organizaciones marítimas. Dado que las organizaciones marítimas son únicas y varían en numerosos aspectos, y que la mayoría de los marcos normativos nacionales pertinentes están aún en fase de desarrollo, no existe un conjunto de directrices y recomendaciones que sirva para todo. En cambio, las organizaciones marítimas deben aplicar las mejores prácticas en función de su entorno operativo, sus recursos financieros y su capacidad de riesgo.

Las organizaciones marítimas de todo el mundo, incluidas las del hemisferio occidental, continúan avanzando hacia una mayor digitalización y automatización. Este documento se propone ayudar a las organizaciones marítimas del hemisferio occidental a cerciorarse de que sus capacidades de gestión de riesgos cibernéticos crezcan y se adapten a su creciente competitividad y eficiencia.



# 2.0

## EL RIESGO CIBERNÉTICO EN EL ÁMBITO MARÍTIMO

### 2.1 Por qué la seguridad cibernética es importante para los puertos del hemisferio occidental

Las organizaciones marítimas desempeñan una función esencial en el hemisferio occidental porque facilitan las actividades de la cadena de suministro nacional e internacional conectando los servicios de transporte marítimo y terrestre. Según IHS World Trade Service, el comercio marítimo en el hemisferio occidental asciende aproximadamente a 3,75 billones de dólares<sup>4</sup>, y el valor económico combinado de las actividades portuarias es mucho mayor. El hemisferio occidental incluye un gran número de puertos e instalaciones marítimas importantes (por ejemplo, el Canal de Panamá) en diversos niveles de desarrollo tecnológico, y el bienestar de algunos países, incluso del Caribe, depende en buena medida de la eficiencia de los puertos y del tráfico de contenedores de carga.

Los países de la región están digitalizando cada vez más sus operaciones logísticas marítimas y adoptando nuevas tecnologías, como la implementación de sistemas comunitarios portuarios<sup>5</sup> (por ejemplo, en Perú y Jamaica) y la adopción de sistemas de ventanilla única marítima (por ejemplo, en Panamá y Antigua y Barbuda). Estos sistemas están diseñados para ayudar a simplificar la información en los puertos y a procesarla con mayor rapidez. Además, la pandemia de 2020, que tuvo efectos generalizados en las economías latinoamericanas, está acelerando esta tendencia a la digitalización, ya que los Estados están empezando a digitalizar rápidamente muchos procesos, como los permisos, las licencias y las solicitudes de servicios sociales. Si se ignoran las amenazas cibernéticas, se ponen

en peligro estos avances, así como la salud económica y la viabilidad de los operadores portuarios y otras organizaciones marítimas.

Reconociendo estos riesgos, los 34 Estados Miembros de la Organización de los Estados Americanos (OEA) han tomado medidas para mejorar las políticas de seguridad cibernética en todos los sectores, incluido el marítimo. La OEA apoya estos esfuerzos a través de sus programas de seguridad cibernética y seguridad marítima. Estos programas son multifacéticos y se centran en el desarrollo de políticas, el fortalecimiento de capacidades (por ejemplo, mediante capacitación y prácticas), la investigación y la difusión a los Estados. El Comité Interamericano contra el Terrorismo (CICTE) se ha enfocado a identificar las amenazas a las infraestructuras críticas de la región en general. En particular, el Programa de Seguridad cibernética del CICTE ayuda a los Estados Miembros de la OEA a desarrollar estrategias nacionales o regionales de seguridad cibernética, y el Programa de Protección Marítima y Portuaria del CICTE está orientado a ayudar a los Estados a desarrollar estrategias nacionales de seguridad marítima. En conjunto, estas iniciativas establecen los cimientos para abordar los riesgos y vulnerabilidades de la seguridad cibernética marítima en la región.

En los últimos diez años, por ejemplo, trece países del hemisferio occidental, con ayuda del CICTE, han adoptado estrategias nacionales de seguridad cibernética. Estos planes nacionales suelen sentar las bases de políticas para abordar los riesgos cibernéticos en los sectores de infraestructuras críticas, incluido el marítimo. Además, en los últimos cinco años el CICTE ha venido operando una red de intercambio de información denominada “CSIRTAmericas”<sup>6</sup> para ayudar a los países a compartir información y coordinar respuestas rápidas 24 horas al día, 7 días a la semana, a las amenazas y vulnerabilidades de seguridad cibernética. En este sentido, se está elaborando un informe que describe este modelo de intercambio de información y aborda sus cinco pilares: comunidad, taxonomía, nivel de información, canales de comunicación y protocolo de semáforos (TLP). Además, el CICTE también lleva a cabo ejercicios de gestión de crisis de seguridad cibernética, incluido uno realizado en Panamá adaptado a los riesgos de seguridad cibernética de su sector marítimo.

A medida que estos esfuerzos se desarrollan a nivel regional, es necesario prestar más atención a la forma en que las autoridades marítimas pueden implementar medidas operativas para hacer frente a los riesgos de seguridad cibernética en el día a día. Antes de abordar las medidas que pueden tomar esas autoridades, puede ser útil dar un paso atrás y analizar dos factores clave que convierten a las organizaciones marítimas en blancos atractivos para los ataques cibernéticos en todo el mundo: (1) la digitalización y automatización de las operaciones portuarias y marítimas y (2) las organizaciones marítimas como centros y depósitos de datos logísticos.





### 2.1.1 Digitalización y automatización de las operaciones portuarias y marítimas

Las operaciones portuarias y marítimas son complejas e implican una amplia variedad de activos fijos, tecnológicos y de comunicación que se interconectan para apoyar una serie de operaciones de buques, manipulación de carga, cadena de suministro y servicios gubernamentales. A medida que las organizaciones marítimas del hemisferio occidental se digitalizan cada vez más (y en ocasiones se automatizan) para mejorar la eficiencia y la competitividad y, en algunos casos, cumplir con los requisitos nacionales, sus operaciones se vuelven cada vez más vulnerables a las amenazas cibernéticas. Este aumento de la digitalización significa que la vulneración de un activo marítimo o de un grupo de activos marítimos puede tener graves consecuencias para las operaciones, la seguridad, las finanzas y la reputación de una organización marítima. Además, dado que estas organizaciones están cada vez más interconectadas, como ocurre con la creciente adopción de los sistemas comunitarios portuarios, la vulneración de los activos de una organización marítima puede llevar a comprometer los activos de muchas otras.

### 2.1.2 Las organizaciones marítimas como centros y depósitos de datos logísticos

Asimismo, puesto que las organizaciones marítimas sirven como nexos del comercio mundial, se han convertido en centros de información que integran los datos de sus usuarios, como operadores de terminales, transportistas, empresas de logística y autoridades gubernamentales, entre otros. Como centros de datos e información, las organizaciones marítimas crean, procesan, transmiten, reciben y almacenan una gran variedad de datos e información en sus redes y sistemas. Estos datos son comercialmente valiosos para muchos, incluidos los competidores que desean obtener una ventaja o los delincuentes que buscan robar datos o comprometerlos para facilitar las transacciones fraudulentas o el contrabando. Además de garantizar la seguridad digital de sus operaciones, las organizaciones marítimas deben proteger la confidencialidad, integridad y disponibilidad de los datos que residen en sus redes y sistemas, como ocurre con otros centros de transporte, como los aeropuertos.



## 2.2 De qué manera son vulnerables los puertos y los buques

El número de ataques cibernéticos sigue creciendo en una gran variedad de sectores<sup>7</sup> y el sector marítimo no es la excepción: durante el primer semestre de 2020, los ataques cibernéticos a este sector se cuadruplicaron<sup>8</sup>. Las organizaciones marítimas son especialmente vulnerables a los ataques cibernéticos debido a varios factores, entre ellos:

- La creación, el acceso, el procesamiento, el almacenaje y la transmisión de una cantidad importante de datos electrónicos con diversos niveles de protección.
- La facilitación de un gran número de transacciones financieras sustanciales entre una amplia gama de participantes.
- La operación en entornos complejos de tecnologías informáticas y operativas que varían en tamaño y alcance.

Cualquier entorno de red es vulnerable a los ataques cibernéticos y a que la información se vea comprometida. Algunos ejemplos de este tipo de vulnerabilidades son:

- Las condiciones operativas.
- Los factores humanos.
- La interconexión entre puertos y buques.
- La intersección ciberfísica de muchas de sus operaciones.

### 2.2.1 Condiciones operativas

Los entornos operativos de los puertos y terminales marítimos se componen de complejas infraestructuras, organizaciones públicas y privadas y diversos sistemas en red. Los sistemas de control que mueven la carga, la tecnología de reconocimiento óptico que se usa en las grúas y en las puertas de acceso, los dispositivos de identificación por radiofrecuencia (RFID) habilitados para Wi-Fi que reciben los datos de la carga conforme se va escaneando en el puerto y los sistemas de seguridad vinculados a los datos del personal, así como los sistemas operativos de las terminales y los sistemas aduaneros, mejoran el flujo del comercio marítimo internacional. Este aumento de la digitalización ha generado importantes eficiencias para las organizaciones marítimas.

Desgraciadamente, esta conectividad tecnológica crea vulnerabilidades cibernéticas. Las organizaciones marítimas presentan blancos atractivos para los actores de las amenazas cibernéticas porque hay muchas partes interesadas y redes que operan en terminales con un complejo entorno de tecnologías informáticas y operativas. Muchas organizaciones marítimas cuentan con sistemas informáticos que dan soporte a todos los aspectos de la organización, incluidas sus actividades operativas críticas, como la manipulación de la carga y el trasvase y almacenamiento de combustible. Muchas, pero no todas, utilizan tecnologías poco seguras o sistemas antiguos y no actualizados, conectados con otros sistemas, lo que puede aumentar las vulnerabilidades cibernéticas. De este modo, una organización marítima puede



ser un vector de amenazas cibernéticas “de uno a muchos” para sus interesados. Una entidad potencialmente puede exponer a terceros que operan en el entorno de la terminal, incluidos los operadores de la terminal, las autoridades portuarias, los funcionarios de aduanas, las empresas de logística, los agentes, los representantes de los proveedores y muchos otros. Cada una de estas partes interesadas puede tener distintos niveles de gestión de riesgos cibernéticos, y un eslabón débil puede romper la cadena de seguridad cibernética. Esto es particularmente cierto en el caso de los actores marítimos que operan en comunidades portuarias que emplean un sistema comunitario portuario que conecta a numerosos miembros de la comunidad portuaria en un sistema electrónico único e integrado.

Asimismo, a diferencia de los entornos de red de oficina, los dispositivos de control de supervisión y adquisición de datos (SCADA) o las infraestructuras marítimas gestionadas por sistemas de control industrial que se vean comprometidos podrían provocar daños ambientales, pérdidas de bienes de terceros y lesiones físicas o muertes. Adicionalmente, los ataques exitosos que resultan en la divulgación no autorizada de información confidencial o sensible de terceros pueden generar consecuencias en materia de políticas y de observancia de las leyes que pueden conducir a multas y demandas.



## 2.2.2 Vulnerabilidades humanas

Además de estas vulnerabilidades descritas anteriormente, las organizaciones marítimas, al igual que otras organizaciones, enfrentan vulnerabilidades debidas a factores humanos. No obstante, las organizaciones marítimas se enfrentan a retos relacionados con el factor humano debido a la gran variedad de funciones administrativas y operativas que desempeña su personal.

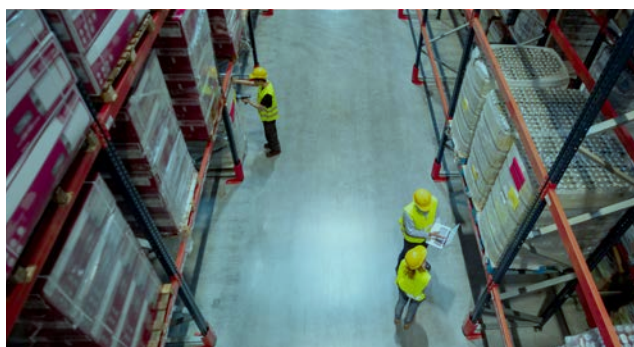
El personal administrativo se relaciona con los puntos finales de la red informática de la empresa, como sus computadoras, impresoras y servidores, a través de los cuales fluyen datos sensibles de la empresa. Así pues, este personal puede ser blanco de estafas de phishing u otras maniobras de ingeniería social.

El personal operativo trabaja en entornos conectados a redes, como los sistemas de manejo de carga con Wi-Fi, los escáners móviles y el control de puertas acceso. También trabaja con complejos sistemas de control industrial críticos que prestan servicio a los buques (como grúas y sistemas de transporte) y necesitan gestionar y hacer funcionar de forma eficiente sistemas cada vez más complejos sin dejar de mantenerse atentos a las amenazas cibernéticas. De la misma manera, los sistemas de tecnología operativa en entornos de terminales complicados son especialmente vulnerables a los errores humanos, ya que un operador descuidado o sin experiencia o un procedimiento demasiado complicado pueden dar lugar a la filtración de información sensible que podría caer en manos de un atacante. Además, los procesos automatizados de manejo de carga que se integran con sistemas de planificación de recursos empresariales (ERP) que se manejan en las oficinas podrían verse comprometidos, lo que daría lugar a violaciones de datos más grandes.

Las organizaciones marítimas pueden aplicar diversas tecnologías y herramientas de



protección. Sin embargo, los empleados que acceden a esas redes pueden tener una variedad de experiencias propias, educación, conocimientos y conductas en materia de seguridad cibernética, por lo que podrían constituir un riesgo cibernético. Algunos empleados pueden representar riesgos cibernéticos por negligencia, por violar involuntariamente las políticas de seguridad o con intenciones maliciosas, como el robo de datos de la organización. Estas vulnerabilidades (conocidas como amenazas internas) exigen que todo el personal, incluidos los altos cargos, reciban capacitación sobre los riesgos cibernéticos (véase la sección 5.2.1).



### 2.2.3 Interconexión entre puertos y buques

Como parte de sus circunstancias operativas, las organizaciones marítimas se enfrentan a vulnerabilidades únicas debido a los buques a los que prestan servicio, que son conductos o portadores potenciales de riesgos cibernéticos. Esto es resultado de varios factores específicos de los buques, entre ellos que son entidades multinacionales, a menudo con regulación relativamente ligera y muy móviles. Por ello, cuando están atracados en un puerto, pueden traer consigo muchos de los riesgos de seguridad de los puertos que han visitado anteriormente. Estos riesgos pueden incluir:

- Posible infección de los sistemas del buque, como los sistemas de navegación, o el uso de los sistemas del buque para transmitir amenazas cibernéticas de escalas anteriores en otros

puertos. Los sistemas de los buques pueden infectarse mediante la introducción involuntaria de virus y otras amenazas cibernéticas por parte de los tripulantes con malas prácticas de seguridad cibernética, como abrir correos electrónicos infectados con malware o utilizar dispositivos USB infectados.

- Equipo en el buque diseñado para recoger y entrar en los sistemas de información del puerto o del gobierno como forma de espionaje.

Además, las organizaciones marítimas en tierra están cada vez más integradas con los buques, ya que estos y los puertos suelen utilizar comunicaciones digitales para intercambiar información. Debido a esta integración, las organizaciones marítimas deben conocer las formas en que los buques pueden actuar como portadores de amenazas cibernéticas contra otras organizaciones marítimas. Un ejemplo significativo fue una campaña de amenazas cibernéticas conocida como “Daily Show”. Este ataque comenzó como un ataque de phishing (véase la sección 5.2.4) contra el capitán de un buque tanque. Desde entonces, el malware ha infectado buques, instalaciones portuarias de petróleo y gas, fábricas, agencias aduanales, empresas de logística y bancos de todo el mundo, incluidos lugares de México y Panamá<sup>9</sup>.



## 2.2.4 Intersección ciberfísica

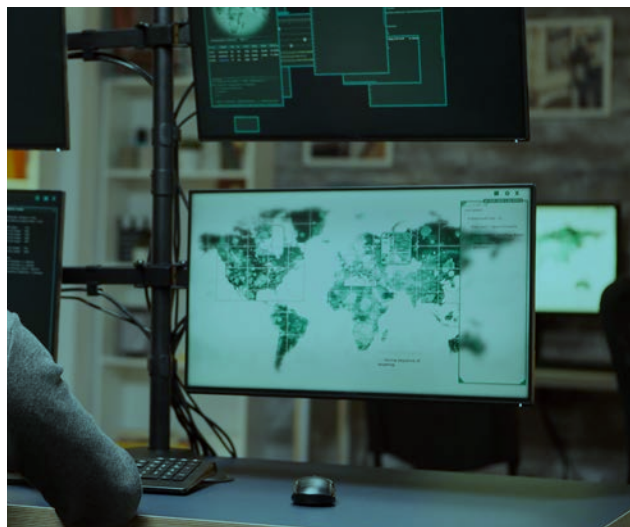
Las organizaciones marítimas han ido transitando de operaciones manuales o con equipos no digitales a la prestación de una serie de servicios portuarios con distintos niveles de procesos y tecnologías integrados, digitales y automatizados. Un factor que impulsa tanto la evolución como la complejidad de las amenazas cibernéticas es la conectividad entre los siguientes sistemas:

- Sistemas basados en tecnologías informáticas, como el control de acceso y las aplicaciones de planificación de recursos empresariales.
- Sistemas orientados al conocimiento del terreno, como los sistemas integrados de vigilancia de la seguridad, incluidos el vídeo, el RADAR y los sistemas de identificación automática.
- Sistemas basados en tecnologías operativas, como los sistemas de control industrial, sistemas habilitados con control de supervisión y adquisición de datos y sistemas de manipulación de cargas, almacenamiento y distribución de transferencia de líquidos a granel, sensores ambientales, etc.

Estos sistemas suelen estar segregados como una práctica óptima. Sin embargo, muchas organizaciones marítimas siguen conectando redes habilitadas con tecnologías informáticas que soportan los sistemas empresariales o de seguridad a las redes de los sistemas de control<sup>10</sup>. A medida que más organizaciones marítimas conectan estos sistemas a las redes, y tratan de adoptar aún más las tecnologías basadas en el Internet de las cosas, surgen nuevas vulnerabilidades que los agentes de amenazas pueden explotar. En particular, este es el caso de las redes informáticas que se conectan a sistemas habilitados con control de supervisión y adquisición de datos y los sistemas de control

industrial que intervienen en la manipulación de la carga, la transferencia y almacenamiento de combustible y los sistemas de gestión de edificios. Por ejemplo, los actores de amenazas cibernéticas podrían utilizar los controles digitales para manipular los sistemas físicos y, por ejemplo, dañar o corromper el sistema operativo de una grúa y dejarla inoperable. En el contexto marítimo, esto podría implicar una vulneración de los controladores lógicos programables que puede sobrepresurizar la infraestructura de tuberías de líquidos a granel y generar un fallo catastrófico que podría poner en peligro la salud y la seguridad del personal o afectar a toda una comunidad portuaria<sup>11</sup>.

Los actores de amenazas cibernéticas han aprovechado esta convergencia entre tecnologías informáticas y operativas en varios ataques a gran escala contra numerosas organizaciones del sector privado. Uno de ellos incluyó el acceso pirata a los sistemas comerciales de una empresa naviera en tierra para planificar con antelación un ataque a un buque. Posteriormente, los asaltantes detuvieron la embarcación en el mar, la abordaron, identificaron la carga que estaban buscando, la localizaron y luego escaparon con ella sin más incidentes<sup>12</sup>. Para ejemplos adicionales de la manifestación física de los ataques cibernéticos, véase el estudio de caso de NotPetya en la sección 2.3.2.



## 2.3 Amenazas de seguridad cibernética

### 2.3.1 Tipos de actores de las amenazas cibernéticas

#### Competidores:

Los competidores poco éticos que buscan explotar las vulnerabilidades cibernéticas pueden contratar atacantes cibernéticos para obtener datos de pago, datos de movimientos y posiciones de la carga, contratos, información confidencial de los clientes, estrategias y actividades de fusión y adquisición, información personal de los empleados y otra información confidencial. Esta información puede permitir que se conozcan las operaciones de la organización y los procesos de toma de decisiones, entre otras cosas, lo que ofrece posibles ventajas a los competidores poco éticos.

#### Los Estados:

Los ataques cibernéticos se están convirtiendo en un arma para los gobiernos que buscan defender la soberanía nacional y proyectar el poder nacional. Los ataques patrocinados por Estados pueden tener consecuencias físicas, económicas y de seguridad. Se sabe que las infraestructuras críticas contienen datos sensibles y son cruciales para las economías. Las organizaciones marítimas, como los puertos, han sido blanco de ataques cibernéticos patrocinados por Estados nacionales<sup>13</sup>.

#### La delincuencia organizada:

La actividad de la delincuencia organizada transnacional basada en el mar sigue siendo un tema que preocupa a los organismos internacionales<sup>14</sup>. Los grupos criminales han logrado vulnerar las redes y los sistemas de los puertos (véase la sección 2.3.2.1). Al obtener acceso a los sistemas de gestión de la carga y la logística, los delincuentes organizados pueden acceder, ver y manipular información sensible sobre la carga, lo que les permite reducir el riesgo de inspección aduanera de determinado envío o incluso robar contenedores enteros.

#### Amenazas internas:

Las organizaciones marítimas se enfrentan a riesgos de seguridad cibernética por parte de empleados actuales, exempleados, contratistas, socios y proveedores. Estas amenazas surgen tanto de acciones intencionales como involuntarias. Las amenazas internas intencionales pueden provenir de un antiguo o actual empleado descontento que tiene posibilidad de usar credenciales no revocadas. Los empleados también podrían ser susceptibles de ser sobornados o chantajeados por terceros para que revelen información sensible, inserten programas maliciosos o incluso reconfiguren protocolos, procesos y configuraciones de tecnologías informáticas y operativas. Los empleados también pueden descargar software malicioso desde correos electrónicos falsos o sitios web infectados sin darse cuenta.

**LAS ORGANIZACIONES MARÍTIMAS ENFRENTAN AMENAZAS DE UNA AMPLIA VARIEDAD DE ACTORES DE AMENAZAS CIBERNÉTICAS**

#### Terroristas:

Aunque el sector marítimo ha tomado medidas importantes para reforzar sus operaciones contra la amenaza de ataques terroristas físicos a las instalaciones y otras infraestructuras críticas, las organizaciones marítimas siguen siendo vulnerables a la nueva amenaza del ciberterrorismo. Los puertos clave u otras infraestructuras marítimas críticas, como el Canal de Panamá, pueden ser blancos atractivos para los terroristas en el hemisferio occidental.

#### Hackers y hacktivistas:

Individuos o pequeños grupos con conocimientos especializados, habilidades únicas y experiencia que pueden facilitar el robo cibernético de dinero o bienes que pueden vender. En ocasiones los hackers contratan sus servicios a otros actores de amenazas cibernéticas, como grupos delictivos organizados, gobiernos o incluso empresas privadas que buscan una ventaja competitiva. Algunos hackers están motivados más por la ideología que por el beneficio económico. Estas personas se denominan "hacktivistas" y utilizan medios cibernéticos para promover agendas o causas políticas, ya sea de forma independiente o a través de una organización más grande.



## 2.3.2 Estudios de casos

En los últimos años se han producido numerosos ataques cibernéticos exitosos contra organizaciones marítimas y los miembros de su comunidad. Los estudios de casos de esta sección ilustran los diferentes tipos de ataques a los que pueden enfrentarse las organizaciones marítimas: los dirigidos a toda una comunidad portuaria, los que buscan maximizar la destrucción y los que son intentos oportunistas de obtener beneficios económicos.

### 2.3.2.1 Ataques a las comunidades portuarias

Entre 2011 y 2013, los comunicados de prensa indican que un grupo de delincuencia organizada con sede en los Países Bajos reclutó a piratas informáticos para vulnerar los sistemas informáticos del Puerto de Amberes que controlaban el movimiento y la ubicación de los contenedores<sup>15</sup>. Los atacantes penetraron los límites físicos de seguridad mediante intimidación física de los empleados de las instalaciones de la terminal. Una vez que lograron ingresar físicamente a las oficinas administrativas, conectaron keyloggers a los dispositivos de red para obtener visibilidad de los sistemas con datos críticos. Lo hicieron para ocultar cocaína y heroína en cargamentos legítimos, como contenedores de madera y plátanos enviados desde países de América del Sur<sup>16</sup>. Con la ayuda de los piratas informáticos, los delincuentes accedieron a los códigos de liberación de los contenedores seleccionados y obtuvieron conocimiento anticipado de cuándo y dónde enviar un camión para interceptar un contenedor antes de que llegara el propietario legítimo.

Este ataque ilustra cómo las organizaciones marítimas, incluidos los buques, los operadores de terminales y los puertos, no operan de forma aislada, sino dentro de una misma comunidad en la que intercambian y almacenan regularmente datos de una gran variedad de grupos, como las compañías navieras, los agentes de los

transportistas, los operadores de terminales, los transitarios, los agentes de carga, los operadores ferroviarios, el control e inspección de fronteras, el monitoreo del estado de los puertos y las autoridades aduaneras<sup>17</sup>. El ataque cibernético al Puerto de Amberes, fruto de la coordinación y colaboración entre distintos tipos de actores (delincuentes organizados y hackers) que amenazan a las organizaciones marítimas, puso en riesgo los datos de todos los miembros de esa comunidad portuaria.

### 2.3.2.2 Informes sobre ataques provenientes de Estados

Un ejemplo de un importante ataque de seguridad cibernética a un puerto que afectó a la región del hemisferio occidental fue el llamado caso “NotPetya”. En junio de 2017, se reportó en informes gubernamentales<sup>18,19,20</sup> y de medios de comunicación<sup>21</sup> que una ola de ataques cibernéticos perjudiciales se había extendido por todo el mundo y repartido un wiper malware llamado “NotPetya”, que llegó a infectar las operaciones globales de A.P. Moller-Maersk, el mayor operador de buques portacontenedores del mundo<sup>22</sup> y uno de los cinco mayores operadores de terminales portuarias<sup>23</sup>. Las computadoras se infectaron con el malware NotPetya y afectaron las operaciones de 17 terminales portuarias operadas por Maersk, entre ellas las de Callao (Perú), Elizabeth, Nueva Jersey (Estados Unidos), Itajai (Brasil), Los Ángeles (Estados Unidos) y Buenos Aires (Argentina). Maersk se vio obligada a interrumpir sus operaciones a medida que el malware se extendía por los sistemas informáticos críticos y para recuperarse tuvo que modificar casi toda su infraestructura informática<sup>24</sup>. Este ataque tuvo efectos en toda la base de clientes de Maersk, y provocó retrasos incluso en la carga para muchos clientes<sup>25</sup>. En su intervención en el Foro Económico Mundial en enero de 2017, el presidente de Maersk, Jim Hagemann Snabe, señaló que Maersk había reinstalado toda su infraestructura informática y que

había sufrido pérdidas financieras de hasta 300 millones de dólares<sup>26</sup>.

Aunque muchos creyeron inicialmente que NotPetya era un ransomware y que los atacantes buscaban un beneficio económico con el ataque, el objetivo del malware puede haberse centrado en la destrucción<sup>27</sup>. NotPetya, un wiper malware, encriptaba partes clave de las computadoras infectadas, pero no existía ninguna clave para revertir la encriptación. Los gobiernos de muchos países afectados, incluyendo Estados Unidos<sup>28</sup> y el Reino Unido<sup>29</sup>, y organizaciones intergubernamentales como la Organización del Tratado del Atlántico Norte<sup>30</sup>, anunciaron que un actor estatal era responsable de NotPetya. Aunque la destrucción de datos no estaba planeada específicamente en contra de Maersk ni ninguna otra organización marítima, NotPetya fue un recordatorio de que las organizaciones marítimas que operan en el moderno mundo digital pueden ser víctimas de este tipo de ataques cibernéticos.

### 2.3.2.3 Ataques oportunistas

Además de los ataques dirigidos (como Amberes) y los ataques destructivos a gran escala (como NotPetya), las organizaciones marítimas también deben tener cuidado con los ataques oportunistas menos coordinados, pero aun así perjudiciales, que se producen con frecuencia. Estos ataques oportunistas se aprovechan de un blanco vulnerable que el atacante no había identificado previamente. Por ejemplo, varias organizaciones marítimas han sufrido ataques de ransomware, que son ataques oportunistas comunes<sup>31</sup>:

- En 2018, el Puerto de San Diego (Estados Unidos) fue víctima de un ataque de ransomware contra más de 200 entidades públicas y hospitales<sup>32</sup>.
- En 2018, el Puerto de Barcelona (España) sufrió un ataque de ransomware que afectó algunos de sus servidores y sistemas<sup>33</sup>.

- En 2018, la naviera Cosco sufrió un ataque de ransomware que afectó sus sistemas de comunicación en Estados Unidos, Canadá y Sudamérica<sup>34</sup>.

- En 2020, la empresa de logística Toll Group sufrió un ataque de ransomware que afectó muchos de sus sistemas informáticos<sup>35</sup>.

Estas organizaciones marítimas no fueron blanco específico de un ataque como ocurrió con el puerto de Amberes descrito en la sección 2.3.2.1. En cambio, tenían una debilidad o vulnerabilidad que los atacantes estaban explotando como parte de campañas más amplias y se convirtieron en víctimas de estos ataques menos impactantes pero igualmente dañinos.



# 3.0

## REGLAMENTOS Y DIRECTRICES



Para prevenir los tipos de ataques que se describieron arriba, los países, las organizaciones internacionales y las entidades privadas están elaborando normas sobre formas para manejar los riesgos cibernéticos, entre ellas reglas para guiar la gestión y el intercambio de información electrónica sensible, proteger la información personal, notificar las violaciones cibernéticas y reducir otras vulnerabilidades. En esta sección se analiza cómo la Organización Marítima Internacional (OMI)<sup>36</sup>, otros organismos multilaterales y los Estados están elaborando normas relativas a la seguridad cibernética que son específicas o atañen al sector marítimo.



# 3.1 Intentos internacionales para abordar las cuestiones de la seguridad cibernética marítima

## 3.1.1 La OMI y el transporte marítimo

La OMI, la principal organización marítima internacional, apenas recientemente ha comenzado a abordar las consideraciones de seguridad cibernética en el ámbito marítimo con cierto nivel de especificidad. En 2017 aprobó una resolución y publicó orientaciones específicas sobre la seguridad cibernética de los buques<sup>37</sup>. Esta resolución exige a los propietarios y gestores de buques que incorporen la gestión de riesgos cibernéticos a sus sistemas de gestión de la seguridad antes de cierta fecha para cada buque y alienta a las autoridades nacionales a verificar el cumplimiento de este requisito.

Ese mismo año, la OMI complementó esta resolución con sus Directrices sobre la gestión de los riesgos cibernéticos marítimos<sup>38</sup>. Estas directrices proporcionan recomendaciones de alto nivel sobre la gestión de los riesgos cibernéticos marítimos. En ellas se reconoce que las tecnologías cibernéticas son esenciales para el funcionamiento y la gestión de los sistemas críticos para la seguridad del transporte marítimo y la protección del medio ambiente marino y que las organizaciones marítimas son vulnerables a los riesgos cibernéticos, por lo que deben analizar las maneras en que se accede a sus sistemas, las formas en que se interconectan entre sí y cómo se conectan en red. Estas directrices se alinean estrechamente con directrices similares adoptadas por Estados Unidos en el “Marco de Seguridad Cibernética” del Instituto de Nacional de Estándares y Tecnología (NIST CSF), que se analizan en la sección 3.3.

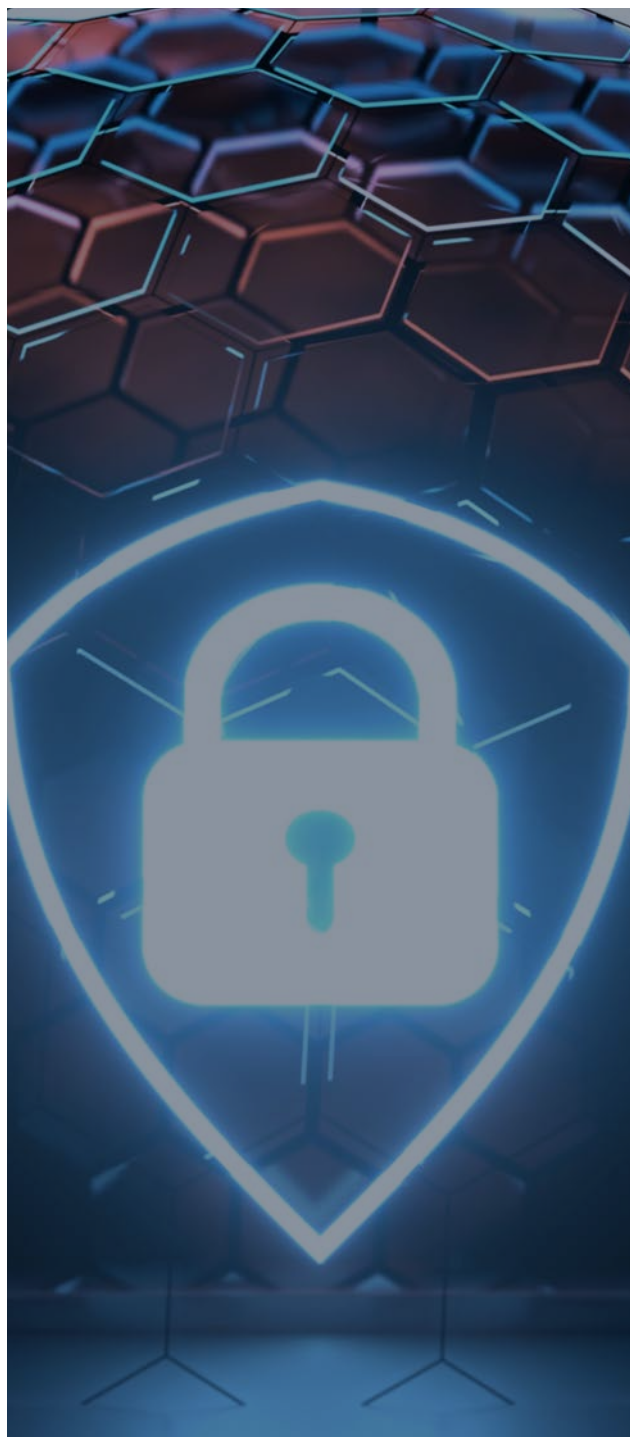
### 3.1.2 La OMI y los puertos

Hasta la fecha, la OMI no ha adoptado medidas orientadas específicamente a la seguridad cibernética de las instalaciones portuarias (a diferencia de las medidas anteriores, que se enfocan en los buques). Sin embargo, en junio de 2020 emitió una circular en la que respalda el llamamiento a la acción del sector encabezado por la Asociación Internacional de Puertos y Terminales para impulsar el crecimiento de la digitalización del sector marítimo y logístico que incluyó la necesidad de hacer frente a los riesgos cibernéticos en los puertos.

Sin embargo, las autoridades portuarias tienen cierta obligación de abordar la seguridad cibernética, incluso en ausencia de una resolución específica de la OMI sobre el tema. Por ejemplo, las instalaciones portuarias sujetas al Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP) deben tener en cuenta las amenazas cibernéticas como parte de su observancia de este código. El Código PBIP forma parte del Convenio para la Seguridad de la Vida Humana en el Mar (SOLAS), que establece disposiciones mínimas de seguridad para los buques, los puertos y los organismos gubernamentales.

Para cumplir con las disposiciones normativas del Código PBIP, las instalaciones portuarias deben llevar a cabo una evaluación de la protección de la instalación portuaria, elaborar un plan de protección de la instalación portuaria, nombrar un oficial de protección de la instalación portuaria e invertir en determinados equipos de protección. Las evaluaciones de la protección de las instalaciones portuarias deben incluir la identificación de las posibles amenazas a los activos e infraestructuras y la probabilidad de que se produzcan, con el fin de establecer y priorizar las medidas de seguridad. Las amenazas cibernéticas son cada vez más frecuentes, por lo que identificar e incluir las consideraciones de seguridad cibernética en las evaluaciones de la protección de las instalaciones portuarias sería

una forma ideal para que las organizaciones marítimas comenzaran a abordar estas cuestiones cruciales. Junto con el desarrollo de estrategias nacionales de seguridad cibernética, estas son vías prácticas para que los Estados desarrollen un marco legal y práctico para hacer frente a estos desafíos.





## 3.2 Legislaciones y normativas nacionales

Actualmente la legislación nacional específica para el sector marítimo en materia de seguridad cibernética es mínima, incluido el hemisferio occidental. No obstante, los puertos y otras infraestructuras marítimas están cubiertos por algunas estrategias nacionales de seguridad cibernética y por legislación general de seguridad cibernética nacional y multilateral.

### 3.2.1 Estrategias nacionales de seguridad cibernética

Para finales de 2020, un total de trece (13) países de todo el hemisferio occidental han desarrollado estrategias nacionales de seguridad cibernética y siete (7) están actualmente en fase de desarrollo con el apoyo del CICTE/OEA<sup>39</sup>. Las estrategias de seguridad cibernética definen específicamente la protección cibernética de las infraestructuras críticas, incluidos los puertos, como uno de sus objetivos centrales. Debido a su papel fundamental en las economías modernas, los puertos se consideran en general como infraestructuras básicas. En consecuencia, deben asegurarse de que sus estrategias de seguridad cibernética estén alineadas con sus funciones y responsabilidades establecidas en las estrategias nacionales de seguridad cibernética pertinentes.

### 3.2.2 Legislación nacional y supranacional y normativa multilateral

Varios países y organismos multilaterales disponen de directivas y otros lineamientos centrados en los puertos y sus responsabilidades en materia de seguridad cibernética como infraestructuras críticas. Las directivas y lineamientos que se destacan a continuación, aunque están orientados principalmente a los puertos de la jurisdicción de cada entidad, siguen siendo útiles para los puertos fuera de su jurisdicción. Entre ellos se incluyen:

- **La Circular de Navegación e Inspección de Buques 01-20, de Estados Unidos: “Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities”.** En 2020, Estados Unidos publicó la Circular de Navegación e Inspección de Buques (NVIC) 01-20 con directrices para abordar los riesgos cibernéticos en las instalaciones reguladas por la Ley de Seguridad del Transporte Marítimo, que proporciona orientación a los propietarios y operadores de instalaciones sobre el cumplimiento de los requisitos para evaluar, documentar y abordar las vulnerabilidades de los sistemas informáticos y redes. En esta circular, la Guarda Costera de Estados Unidos (USCG) adopta la postura de que los propietarios y operadores de instalaciones portuarias están obligados, en virtud de la Ley de Seguridad del Transporte Marítimo de Estados Unidos de 2002, que implementó el Código PBIP en Estados Unidos, a abordar las vulnerabilidades de seguridad cibernética y garantizar la seguridad cibernética de sus instalaciones. Estados Unidos ha anunciado que, a partir del 1 de octubre de 2021, los propietarios y operadores de instalaciones portuarias deberán presentar enmiendas de seguridad cibernética a las evaluaciones y planes que requiere la Ley de Seguridad del Transporte Marítimo de Estados Unidos durante las auditorías. La circular proporciona orientación sobre la manera en que los propietarios y operadores de instalaciones portuarias





pueden cumplir esos requisitos, pero no crea ninguna obligación nueva ni modifica los requisitos que figuran en la normativa vigente<sup>40</sup>. Asimismo, en diciembre de 2020, Estados Unidos publicó un Plan Nacional de Seguridad Cibernética Marítima que requerirá que la USCC desarrolle un marco para las evaluaciones de seguridad cibernética portuaria<sup>41</sup>.

- **La Directiva de Seguridad de las Redes y Sistemas de Información de la Unión Europea.** En 2016, el Parlamento Europeo adoptó la Directiva de Seguridad de las Redes y Sistemas de Información (Directiva NIS), que ayuda a los operadores de infraestructuras críticas a crear programas de seguridad cibernética que puedan prevenir, detectar, notificar a las autoridades y responder adecuadamente a los incidentes de seguridad. La Directiva NIS clasifica como operadores de servicios esenciales a los organismos gestores de los puertos, incluidas sus instalaciones portuarias, así como a las entidades que operan con las obras y equipos que se encuentran en los puertos. Por lo tanto, como operadores de servicios esenciales, estas organizaciones están sujetas a los requisitos de la Directiva NIS, incluida la realización de evaluaciones de riesgo, que abarcan, entre otras cosas, la seguridad, la integridad y la resiliencia de las redes y los sistemas de información<sup>42</sup>.

- **La Ley de seguridad cibernética de Singapur.** En 2019, Singapur aprobó la Ley de seguridad cibernética de Singapur, que establece un marco legal para la supervisión y el mantenimiento de la seguridad cibernética en ese país. Esta ley exige que las organizaciones de los sectores de infraestructuras críticas de la información prevengan, gestionen y respondan a las amenazas e incidentes

de seguridad cibernética, protejan las infraestructuras críticas de información y compartan la información sobre estas infraestructuras con la Agencia de Seguridad Cibernética de Singapur en caso de un ataque cibernético. La infraestructura de transporte marítimo está incluida en la definición de infraestructura de información crítica.



## 3.3 Marcos políticos y normas industriales útiles

Como se ha señalado anteriormente, existen pocos marcos legislativos nacionales en materia de seguridad cibernética y pocos requisitos multilaterales para abordar las amenazas a la seguridad cibernética marítima. Dicho esto, existen otras referencias que pueden ayudar a las organizaciones marítimas a abordar estas cuestiones y servir como base para el desarrollo de sus capacidades de seguridad cibernética. Las normas y los marcos que se analizarán en esta sección se refieren a las infraestructuras críticas en general (secciones 3.3.1, 3.3.2 y 3.3.3) o a las infraestructuras marítimas en particular (secciones 3.4.1 y 3.4.2)<sup>43</sup>.

### 3.3.1 Marco de Seguridad Cibernética del Instituto de Nacional de Estándares y Tecnologías de Estados Unidos.

El NIST CSF fue uno de los primeros marcos normativos sobre la forma en que las organizaciones pueden evaluar y mejorar su capacidad para prevenir, detectar y responder a los ataques cibernéticos<sup>44,45</sup>. Este marco ofrece una hoja de ruta para las organizaciones, como las instalaciones marítimas, que buscan identificar las vulnerabilidades, las amenazas y las dependencias y desean aplicar las prácticas óptimas para la gestión de los riesgos cibernéticos<sup>46</sup>. El NIST CSF les permite a las organizaciones, independientemente de su tamaño, grado de riesgo de seguridad cibernética o sofisticación de la seguridad cibernética, aplicar los principios y las mejores prácticas de gestión de riesgos para mejorar la seguridad y la resiliencia de las infraestructuras críticas. Desde su lanzamiento, se ha traducido a múltiples idiomas, incluidos el español y el portugués, y lo han adoptado numerosos países, como Italia, Japón, Arabia Saudita, Suiza y Uruguay<sup>47</sup>.

Tanto las Directrices sobre la gestión de riesgos cibernéticos marítimos de la OMI como la NVIC 01-20 de la USCG se basan en el marco NIST. Este marco consta de cinco áreas funcionales para gestionar el riesgo cibernético en toda una organización como parte de un plan coordinado: Identificar, proteger, detectar, responder y recuperar.



# Marco



## 1 Identificar

Definir las funciones y responsabilidades del personal para la gestión de riesgos cibernéticos e identificar los sistemas, activos, datos y capacidades que plantean riesgos para las operaciones comerciales de las empresas e instalaciones marítimas si se interrumpen.



## 2 Proteger

Implementar procesos y medidas de control de riesgos (incluyendo medidas técnicas) y planes de contingencia para protegerse contra un evento cibernético y garantizar la continuidad de las actividades administrativas y operativas marítimas.



## 3 Detectar

Desarrollar e implementar actividades para detectar un evento cibernético de manera oportuna, comunicar los incidentes a las partes interesadas en los entornos administrativos y operativos y garantizar la comunicación expedita a las partes interesadas de la comunidad portuaria y de la carga, cuando corresponda.



## 4 Responder

Desarrollar y poner en práctica actividades y planes para la resiliencia y la restauración de los sistemas cuando los eventos cibernéticos perjudican las operaciones o los servicios marítimos.



## 5 Recuperar

Identificar medidas para respaldar y restaurar los sistemas necesarios para las operaciones marítimas afectadas por un evento cibernético, incluyendo la coordinación y el trabajo con partes interesadas externas, según sea necesario.



### 3.3.2 Normas 27000 y 28000 de la Organización Internacional de Normalización

El conjunto de normas de la Comisión Electrotécnica Internacional de la Organización Internacional de Normalización está diseñado para ayudar a proteger los activos de información, que incluyen la propiedad intelectual, los datos sensibles de los empleados o clientes y la información financiera en una serie de sectores. Aunque existen numerosas normas de la serie 27000, la más conocida es la 27001, que presenta los requisitos de un sistema de gestión de la seguridad de la información. Un sistema de gestión de la seguridad de la información es un marco de gestión que se emplea para identificar y evaluar el riesgo de la información y adaptarse y evolucionar para hacer frente a los cambios en las amenazas y vulnerabilidades cibernéticas.

Además de la ISO 27001, la ISO 28000:2007 proporciona especificaciones para los sistemas de gestión de la seguridad para la cadena de suministro, incluyendo la seguridad de la información y la garantía de seguridad. Esta norma es útil para organizaciones de todos los

tamaños y rangos de complejidad de tecnologías informáticas y operativas, lo que puede ser útil para las organizaciones marítimas, cuyo tamaño y complejidad en cuanto a tecnologías informáticas y operativas puede variar. También puede ser de especial utilidad para las organizaciones marítimas cuyos fines incluyen garantizar el cumplimiento interno de los objetivos definidos de gestión de la seguridad y medir el progreso de la organización con respecto a los puntos de referencia de las mejores prácticas.

### 3.3.3 Controles del Centro de Seguridad de la Información

Los Controles Críticos de Seguridad para una Ciberdefensa Eficaz del Centro de Seguridad de la Información, conocidos como Controles CIS, son un conjunto de buenas prácticas que las organizaciones pueden aplicar para bloquear o mitigar los ataques conocidos. Estos controles fueron desarrollados originalmente por el Instituto SANS con contribuciones de agencias del gobierno estadounidense y expertos comerciales y son especialmente útiles porque se actualizan continuamente y se nutren de las lecciones aprendidas en materia de ataques.



## 3.4 Directrices del sector

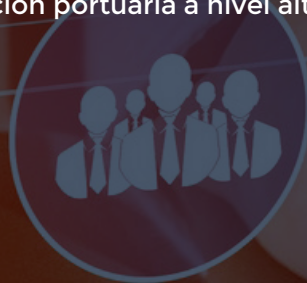
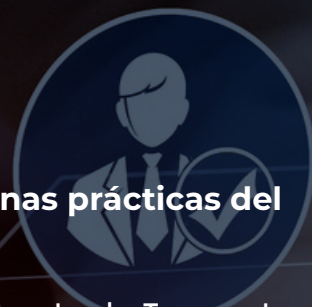
### 3.4.1 Seguridad cibernética portuaria: Buenas prácticas de la Agencia Europea de Seguridad de las Redes y de la Información para la seguridad cibernética en el sector marítimo

Además de las directrices de la OMI y la USCG basadas en el NIST CSF, la Unión Europea ha elaborado una guía de mejores prácticas para los directores de información y los directores de seguridad de la información del sector portuario. En esta guía se identifican los nuevos retos relacionados con las tecnologías informáticas y operativas en el sector portuario, se definen las amenazas a la seguridad cibernética portuaria y se recomiendan las medidas de seguridad que deben implementar los puertos. En ella se identifican las siguientes buenas prácticas:

- Definir una gobernanza clara en torno a la seguridad cibernética, con la participación de todas las partes implicadas en las operaciones portuarias.
- Crear conciencia en los puertos en materia de seguridad cibernética e infundir una cultura de seguridad cibernética.
- Hacer cumplir los fundamentos técnicos de la seguridad cibernética.
- Considerar la seguridad por diseño en las aplicaciones.
- Reforzar las capacidades de detección y respuesta a nivel portuario.

### 3.4.2 Guía de buenas prácticas del Reino Unido

En 2020, el Departamento de Transporte del Reino Unido publicó una iteración actualizada de su Good Practice Guide: Cyber Security for Ports and Port Systems (publicada originalmente en 2016), que proporciona consejos prácticos para llevar a cabo una evaluación y elaborar un plan de seguridad cibernética para los activos importantes, manejar las brechas de seguridad y garantizar el uso de estructuras de gobierno, funciones, responsabilidades y procesos correctos. Esta guía incluye información para llevar a cabo una evaluación de la seguridad cibernética, elaborar un plan de seguridad cibernética y establecer la gobernanza y la gestión de la seguridad cibernética dentro de las instalaciones portuarias. Este nivel de detalle está destinado a los profesionales de la protección portuaria y no a los ejecutivos que supervisan la protección portuaria a nivel alto.





## 3.5 Requisitos de privacidad de los datos

Las leyes de protección de datos están aumentando tanto en número como en amplitud en todo el hemisferio occidental. Es importante que las organizaciones marítimas conozcan (1) el marco jurídico sobre la protección de datos en el país en el que operan y (2) si los datos que procesan están sujetos a las leyes de protección de datos de otros países.

Varios Estados de América Latina han adoptado leyes estrictas de protección de datos que siguen las líneas de la Unión Europea en su influyente Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2018. Un ejemplo de una ley de protección de datos estricta en el hemisferio occidental es la Ley General de Protección de Datos de Brasil, que se aprobó el 9 de julio de 2019 y coincide estrechamente con muchas de las disposiciones del Reglamento General de Protección de Datos, incluidos los derechos de los sujetos de datos, los requisitos para los oficiales de protección de datos y las bases sobre las que se pueden procesar los datos personales<sup>48</sup>. Argentina cuenta con una Ley de Protección de Datos Personales desde el año 2000, pero su Congreso ha debatido un proyecto de ley sustituta que se alinearía cercanamente con el Reglamento General de Protección de Datos, incluyendo en la concesión a los ciudadanos del derecho a obtener una copia de los datos personales en manos de los procesadores y el derecho a que se eliminen sus datos personales una vez finalizado el procesamiento. Por su parte, Panamá promulgó en 2019 una Ley de Protección de Datos que entrará en vigor en 2021 en la que se reconocen derechos similares a los establecidos en el Reglamento General de Protección de Datos, incluyendo el derecho de eliminación de los datos y su portabilidad.

Aunque el Reglamento General de Protección de Datos de la UE está basado en la UE y se aplica a las entidades que operan en ella, también se aplica a cualquier entidad fuera de la UE que maneja datos de los residentes de la UE, independientemente de dónde se procesen<sup>49</sup>. Es significativo que, cuando se ven afectados los derechos de los ciudadanos de la UE, el Reglamento General de Protección de Datos obliga a notificar las vulneraciones cibernéticas a las partes afectadas, además de que establece multas estrictas que pueden ascender a 20 millones de euros o al 4% del volumen de negocios anual de una organización, lo que sea mayor<sup>50</sup>.






Las leyes que rigen la protección de datos y la privacidad –la relación entre la recopilación y el uso de datos por parte de una organización y el derecho de los ciudadanos a controlar cómo se recopila y utiliza su información– se han generalizado en el hemisferio occidental en los últimos años. Debido al aumento de los requisitos legales y políticos sobre la seguridad de la información personal, es aún más importante que las organizaciones marítimas adopten políticas para asegurar la información de forma eficaz.



# **4.0**

## **PASOS INICIALES PARA DESARROLLAR LAS CAPACIDADES DE SEGURIDAD CIBERNÉTICA DE UNA ORGANIZACIÓN**

El manejo de los riesgos cibernéticos y la implementación de un programa de seguridad cibernética eficaz abarcan casi todos los aspectos de una organización marítima. Por lo tanto, la responsabilidad de la gestión eficaz de los riesgos cibernéticos y de la seguridad cibernética comienza en la cúpula de las organizaciones. Las organizaciones marítimas deben:

-  1. Establecer quién es responsable de supervisar todas las actividades de gestión de riesgos cibernéticos y de seguridad cibernética dentro de la organización.
-  2. Definir el personal interno y las partes externas que participan en las actividades de gestión de riesgos cibernéticos y de seguridad cibernética.
-  3. Crear un comité directivo para coordinar y administrar formalmente todas las iniciativas de gestión de riesgos cibernéticos.
-  4. Llevar a cabo una evaluación inicial de base de las capacidades generales de seguridad cibernética de la organización.
-  5. Formular una estrategia de gestión de riesgos cibernéticos y aplicar un plan de gestión de riesgos cibernéticos.

## 4.1 Establecimiento de supervisión

La evaluación y la gestión de los riesgos cibernéticos es todavía un concepto relativamente nuevo para las organizaciones marítimas. Es fundamental que la evaluación y la gestión global de los riesgos cibernéticos estén en manos las personas adecuadas. La supervisión de las actividades de gestión de riesgos cibernéticos debe ser responsabilidad de los propietarios, los miembros del Directorio y los ejecutivos de la organización. Los propietarios y los miembros del Directorio son responsables de evaluar el riesgo cibernético para el capital invertido y de proteger el patrimonio de los inversionistas o contribuyentes y los ejecutivos son responsables de evaluar el riesgo cibernético para el rendimiento financiero y la viabilidad operativa de la organización. Como parte de la evaluación, los propietarios, los miembros del Directorio y los ejecutivos deben asegurarse de que la organización defina correctamente a las partes interesadas en materia cibernética y establezca un comité directivo de seguridad cibernética, como se describe en las siguientes subsecciones.

## 4.2 Definición de las partes interesadas

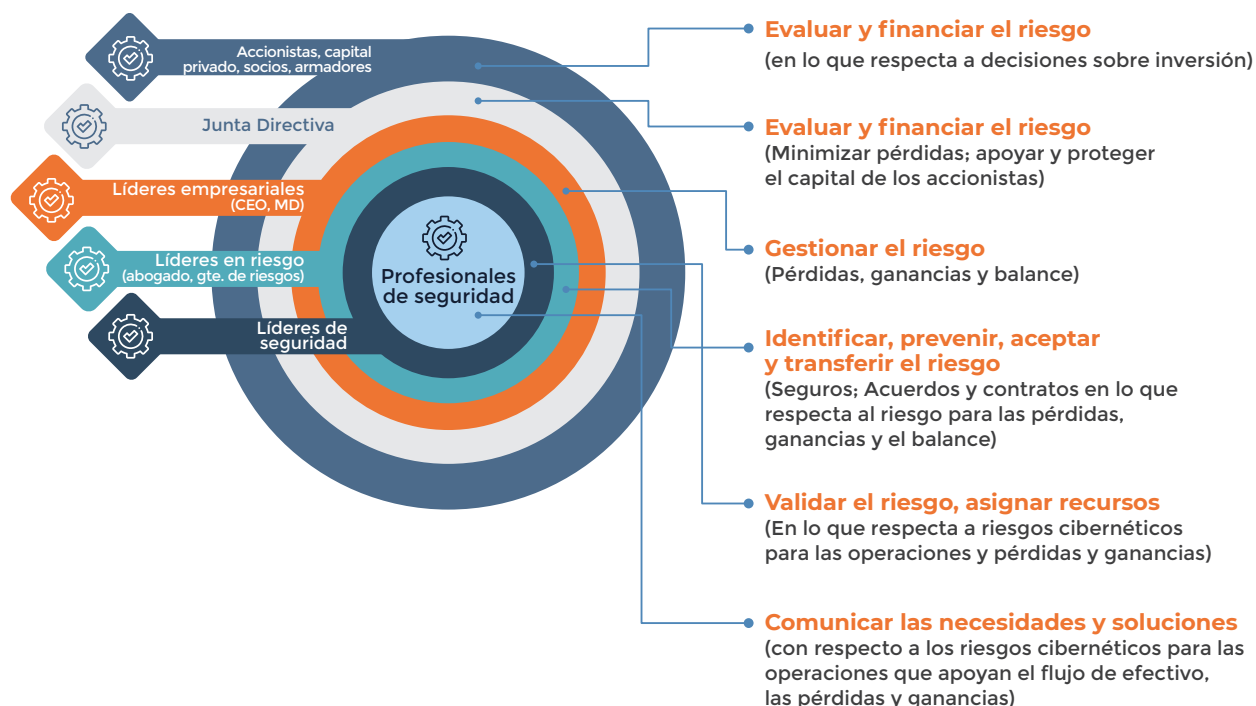
Uno de los pasos iniciales más importantes que puede dar una organización marítima es definir a las partes interesadas en materia cibernética. Aunque no hay dos organizaciones marítimas iguales en el mundo, cada una comparte un universo relativamente común de partes interesadas clave. En la mayoría de los casos, esto incluye a representantes tanto del gobierno como del sector comercial. La parte gubernamental incluye a las autoridades estatales de control portuario y contrataciones, las autoridades portuarias, aduanas e inmigración, control fronterizo, aplicación de la legislación nacional y local, el ejército y otros organismos gubernamentales, incluidos los de medio ambiente, impuestos, salud y seguridad. La parte comercial incluye una amplia gama de operadores de terminales de carga (regulados y no regulados), compañías navieras, agentes marítimos, proveedores de logística, transitarios, operadores de ferrocarril y carretera, operadores de almacenes, estibadores, empresas de reparación y mantenimiento de buques, empresas de servicios públicos, empresas de petróleo, gas y afines, empresas de telecomunicaciones y diversas empresas de servicios y consultoría especializados.

Las partes interesadas en materia cibernética dentro de una organización marítima abarcan a todos los empleados administrativos y de operaciones que tienen acceso a los activos digitales para crear, acceder, procesar, almacenar o transmitir datos electrónicos. Incluyen también a los directorios, los inversionistas, los comisarios, los socios, los proveedores, los clientes, todas las partes interesadas gubernamentales y otras personas que participan en estos intercambios de datos, como:

- Jefes de operaciones.
- Directores de tecnología.
- Jefes de seguridad.
- Oficiales de seguridad de las instalaciones portuarias.
- Directores de departamentos como operaciones de carga, gestión de contratos y proveedores, informática, jurídico, salud y seguridad y capacitación.

Adicionalmente, se extienden más allá de estas partes interesadas inmediatas a personas con las que mantienen relaciones personales, que a menudo se comunican con las partes interesadas de la organización y les transmiten datos o reciben información de ellas.





## 4.3 Creación de un comité directivo de seguridad cibernética

Una vez que la organización marítima ha definido a sus partes interesadas en materia cibernética, debe establecer un comité directivo de seguridad cibernética. La función de este comité es supervisar y coordinar las iniciativas de toda la organización destinadas a reducir los riesgos cibernéticos. El comité directivo de seguridad cibernética debe ayudar a conducir la estrategia de gestión de riesgos cibernéticos de la organización, garantizar la coordinación en su aplicación, consolidar la autoridad, reducir las posibilidades de duplicación del gasto en seguridad, controlar y supervisar las inversiones o infraestructuras complejas, agilizar las comunicaciones interfuncionales e impulsar el cambio cultural de la organización en materia de seguridad cibernética. También debe ser responsable de participar continuamente en la identificación, evaluación y mitigación de las vulnerabilidades, en la respuesta a los incidentes, la recuperación y la redacción y en la implementación y actualización de las políticas y procedimientos. El establecimiento de un comité directivo de seguridad cibernética le permite a la organización optimizar las actividades de presupuestación y adquisición, obtener y promover consensos, asignar autoridades e instituir responsabilidad, además de servir como principal impulsor del intercambio de información y del compromiso interfuncional.

El comité directivo de seguridad cibernética debe incluir a las partes interesadas de alto nivel de todas las funciones operativas de la organización marítima. Un equipo multidisciplinar con diversas perspectivas, conocimientos y experiencia será el más capacitado para caracterizar las vulnerabilidades, reconocer las consecuencias e identificar soluciones. Lo ideal es que el equipo de una organización marítima incluya representantes de seguridad, ingeniería y operaciones, tecnologías de la información, salud y seguridad industrial, capacitación, manejo de emergencias, administración, finanzas, asuntos legales, recursos humanos y gestión de riesgos y observancia, entre otros. En algunos casos también pueden participar representantes

de socios críticos, como el arrendatario de una instalación portuaria o un proveedor de servicios externos (como tecnología informática o seguridad).

#### 4.3.1 Estrategias para impulsar el cambio

Un estudio del Foro Económico Mundial de 2014 concluyó que el mayor impulsor de la capacidad de seguridad cibernética de las organizaciones (y, por tanto, de la resiliencia) era el compromiso de los ejecutivos. Esto se validó independientemente del tamaño de la organización, el sector y los recursos asignados<sup>51</sup>. Por lo tanto, además de definir a las partes interesadas y establecer un comité directivo de seguridad cibernética, los líderes de las organizaciones marítimas deben participar activamente en las actividades de gestión de los riesgos cibernéticos de sus organizaciones. Entre las consideraciones importantes para los líderes de las organizaciones marítimas se encuentran:

- **La participación en los procesos de toma de decisiones en materia de gestión de riesgos cibernéticos.** Los líderes en el sector marítimo pueden ayudar a sus organizaciones a determinar qué es lo que está en riesgo en materia cibernética, las tolerancias de riesgo cibernético de la organización y las prioridades de gestión del riesgo cibernético de la organización, considerando las compensaciones entre la aceptación, la evitación, la mitigación y la transferencia (cobertura de seguros) del riesgo.
- **El fomento de la conciencia sobre los riesgos cibernéticos y la participación de todas las áreas funcionales de la organización.** Los líderes en el sector marítimo pueden asegurarse de que todas

las áreas funcionales de la organización, incluyendo operaciones, legal, contratos, adquisiciones, ventas y marketing, relaciones públicas, administración y finanzas, conozcan las actividades de gestión de los riesgos cibernéticos y se comprometan con ellas.

- **El cambio de los comportamientos en la organización.** Los líderes en el sector marítimo pueden demostrar la importancia del comportamiento consciente de los riesgos cibernéticos destacando el valor de la capacitación y las campañas de concientización en materia cibernética. Por ejemplo, pueden hacer hincapié en la importancia del uso cibernéticamente responsable del correo electrónico.
- **La implementación de la gobernanza y la responsabilidad.** Los líderes en el sector marítimo pueden apoyar activamente los esfuerzos para incorporar formalmente las responsabilidades en materia de seguridad cibernética a todas las funciones, definir las autoridades adecuadas e instituir procedimientos bien definidos de notificación para dar seguimiento a los avances hacia los objetivos empresariales.
- **El presupuesto para la gestión sostenida de los riesgos cibernéticos.** Muchas organizaciones incluyen sus presupuestos de seguridad en otros centros de costos<sup>52</sup>. Los líderes en el sector marítimo pueden establecer presupuestos dedicados a la gestión de riesgos cibernéticos que incluyan tanto los gastos de capital como los gastos operativos recurrentes.



## 4.4 Evaluación preliminar de la capacidad de toda la organización

Tras definir el universo de partes involucradas en materia cibernética y establecer un comité directivo de seguridad cibernética, es importante que las organizaciones marítimas conozcan sus capacidades existentes de gestión de riesgos cibernéticos a fin de obtener un planteamiento más estudiado que permita determinar qué medidas pueden adoptarse para mejorar las capacidades de gestión de riesgos cibernéticos de que disponen. Para ello deben realizar una evaluación de la capacidad de seguridad cibernética existente en toda la organización que les ayude a comprender su capacidad para gestionar y mitigar los riesgos cibernéticos y determinar las acciones que se requieren para implementar mejoras o medir los avances con el paso del tiempo.

Una evaluación de la capacidad en materia de seguridad cibernética les permitirá analizar los procesos, el personal y las tecnologías que componen su gestión de riesgos cibernéticos y su postura con respecto a la seguridad cibernética. Mediante esta evaluación podrán identificar y examinar mejor sus deficiencias en materia de seguridad cibernética y determinar la asignación de recursos más eficaz y eficiente para mejorar sus capacidades de seguridad cibernética. Esta evaluación debe cubrir temas como:

- El **marco de gobernanza**, que incluye la participación de los líderes de la organización, la gestión de las políticas de riesgos cibernéticos y la notificación de los riesgos cibernéticos.
- La **huella tecnológica**, que incluye todas las redes corporativas en la sede central, las sucursales, instalaciones satélite y subsidiarias y empresas conjuntas, así como todas las plataformas de red y plataformas digitalmente habilitadas, los sistemas de control críticos y otras tecnologías operativas que apoyan las operaciones diarias, como el manejo de la carga, el almacenamiento y transporte de combustible y el apoyo logístico.
- Las **relaciones y dependencias críticas con socios y con la cadena de suministro**, incluyendo programas de gestión de proveedores, incorporación de requisitos de notificación de incidentes cibernéticos y políticas para compartir información cibernética con terceros importantes.
- Las **prácticas de respuesta a incidentes**, incluyendo planes documentados, relaciones con terceras partes que colaborarán en la respuesta a incidentes y capacitación, simulacros y prácticas.

La comprensión por parte de una organización marítima de sus capacidades y deficiencias existentes en materia de seguridad cibernética servirá como base para formular una estrategia de gestión de riesgos de seguridad cibernética y para implementar y mantener el plan de apoyo con el paso del tiempo. En la siguiente sección se analizarán la estrategia y el plan de implementación.



## 4.5 Estrategia de seguridad cibernética y plan de implementación

Después de su evaluación inicial de seguridad cibernética, la organización marítima puede empezar a formular su estrategia de seguridad cibernética y su plan de implementación.

### 4.5.1 Estrategia de seguridad cibernética

Una estrategia de seguridad cibernética incluye objetivos para la maduración de las capacidades internas de seguridad cibernética tanto en los entornos administrativos como en los operativos y una visión general de las iniciativas que promueven la seguridad cibernética en toda la organización, como la planificación de la inversión para actualizaciones tecnológicas y las iniciativas de capacitación de los empleados. También debe incorporar requisitos normativos, cuando corresponda (véase la sección 3.0).

Es esencial que la estrategia de seguridad cibernética se encuadre dentro de la estrategia operativa general de la organización. Las organizaciones marítimas deben considerar específicamente los objetivos de rendimiento que requieran actividades complejas habilitadas para tecnologías operativas, como las operaciones en terminales, la manipulación de la carga, el almacenamiento y el transporte de combustible, los almacenes y el apoyo logístico. Las consideraciones importantes incluyen:

- **Comprender lo que debe proteger la organización,** que incluye los activos y datos críticos en todos los entornos administrativos y operativos. Por ejemplo, un puerto de contenedores podría dar prioridad a sus grúas de barco a tierra y al sistema que gestiona las operaciones de patio, mientras que una terminal de



líquidos a granel podría dar prioridad a los tanques de almacenamiento y a las tuberías y a los sistemas que operan esos activos. Las organizaciones marítimas también deben determinar qué información crítica reside en sus sistemas, como los datos de tripulaciones o pasajeros y los datos comercialmente sensibles.

- **Comprender el apetito de riesgo de la organización,** que varía dependiendo de factores como la industria, tamaño, objetivos y situación financiera de la organización.
- **Comprender el panorama de amenazas de la organización,** que incluye el conocimiento de los clientes, productos, competidores y posibles motivos de ataque de organización. También es importante identificar los beneficios que podría obtener un atacante de una organización específica (véanse ejemplos de ataques cibernéticos a organizaciones marítimas en la sección 2.3.2).

#### 4.5.2 Plan de seguridad cibernética


Una vez que una organización marítima ha formulado su estrategia de seguridad cibernética, puede elaborar un plan para implementarla. El plan de implementación debe incluir por lo menos los siguientes pasos:

- **Seleccionar un marco alrededor del cual crear el plan.** Las opciones incluyen los marcos descritos en la sección 3.3, como el NIST CSF, la Comisión Electrotécnica Internacional de la ISO/IEC 27001 y los Controles del Centro de Seguridad de la Información. Estos marcos están diseñados para mejorar la gestión del riesgo de seguridad cibernética en organizaciones de cualquier sector o comunidad y son aplicables a las organizaciones marítimas. Los marcos les permiten a las organizaciones –sin importar su tamaño, grado de riesgo cibernético o sofisticación cibernética– aplicar los principios y mejores prácticas de la gestión de riesgos y mejorar la seguridad y la resiliencia de la infraestructura crítica.
- **Identificar todo el hardware, software, equipo, plataformas, usuarios y dependencias clave.** Los activos específicos de las organizaciones marítimas pueden incluir sistemas para la gestión de la carga, operaciones de terminales, supervisión de la seguridad, gestión del tráfico de navíos, manejo de emergencias, controles industriales, comunicaciones, transferencia y almacenamiento de combustible y monitoreo ambiental.
- **Comprender las consecuencias para los activos críticos de los eventos cibernéticos.** Debido a la interconexión de las organizaciones marítimas específicamente y de la industria marítima en general, los eventos cibernéticos en las organizaciones

marítimas pueden transferirse a los sistemas y las áreas de unas a las otras. Por ejemplo, un evento cibernético en la planificación de los recursos empresariales de un puerto podría migrar a un sistema operativo de terminal conectado y después al sistema de una naviera conectado con el sistema operativo de terminal y viceversa.


- **Elaborar un plan para impartir capacitación sobre conciencia cibernética a todo el personal.** Puesto que la amplia mayoría de las violaciones de datos son causadas por errores humanos, con frecuencia las personas son el principal blanco de los ataques cibernéticos<sup>53</sup>. Así pues, cualquier plan de seguridad debe tomar en cuenta la necesidad de capacitación continua para todo el personal para sea consciente de los riesgos cibernéticos (véase la sección 5.2.1).
- **Reevaluar, probar y utilizar bucles de retroalimentación continuamente.** La reevaluación continua de plan de seguridad cibernética le permitirá a una organización marítima perfeccionar su plan de seguridad cibernética para adaptarlo a la evolución de los reglamentos y normas, las respuestas a los incidentes y la recuperación de los incidentes y los resultados de la capacitación y las prácticas, lo que le permitirá a la organización seguir mejorando la madurez de su capacidad general de seguridad cibernética y su capacidad de manejar y mitigar los riesgos cibernéticos.



A person wearing a flight suit is shown from the side, adjusting a strap on a harness. The image is overlaid with a semi-transparent blue filter. The text '5.0 MEJORES PRÁCTICAS' is written in white, bold, sans-serif font on the left side of the image.

# 5.0 MEJORES PRÁCTICAS





# 5.1 Mejores prácticas de gobernanza y política

Como se señaló en la estrategia y el plan de seguridad cibernética en la sección 4.3, todas las organizaciones marítimas deben formular y mantener un conjunto de políticas claramente articuladas para salvaguardar los datos sensibles, proteger su reputación y fomentar el desarrollo de una cultura de conciencia cibernética. A continuación se presenta un resumen exhaustivo de los factores que se deben tener en cuenta en la formulación de la estrategia y el plan; estas directrices son aplicables a las instalaciones marítimas de todo el hemisferio occidental.

## 5.1.1 Seguridad de los datos

Las organizaciones marítimas generan, reciben, procesan, almacenan y transmiten una cantidad significativa de información, que incluye información de las partes interesadas de la comunidad portuaria, de los clientes y de los socios; información bancaria y sobre pagos; registros personales; detalles de contratos; datos de cargas y manifiestos; y datos sobre los sistemas de seguridad. Estas organizaciones deben conocer los datos críticos que tienen, saber dónde se encuentran y asegurarse de que estén protegidos. Como se dijo en la sección 2.1.2, deben tomar medidas para proteger la confidencialidad, la integridad y la disponibilidad de sus datos e información y cumplir con las leyes pertinentes sobre la protección de los datos:

- **Confidencialidad:** Las organizaciones marítimas deben limitar el acceso a los datos y a la información exclusivamente a quienes tienen una responsabilidad concreta en relación con ellos u otra necesidad establecida para que se les otorgue acceso. Las amenazas a la confidencialidad pueden provenir de actores tanto externos como internos que buscan acceder a información sensible, robarla o utilizarla inapropiadamente.
- **Integridad:** Las organizaciones marítimas deben preservar la exactitud de sus datos e información, lo cual incluye

protegerlos contra su modificación o eliminación no autorizadas y crear capacidad para restaurar datos precisos si se pierde la integridad.

- **Disponibilidad:** Las organizaciones marítimas deben garantizar que los datos y la información puedan recuperarse cuando se requieran, lo que incluye proteger los datos contra pérdida, destrucción y negación, en particular en lo que toca a datos sensibles o críticos para las operaciones.

Los pasos para preservar la confidencialidad, integridad y disponibilidad de los datos y la información incluyen:

- **Inventariar y clasificar los datos críticos.** Estos datos abarcan tanto los administrativos como los de operaciones críticas. Para las organizaciones marítimas, los datos administrativos críticos pueden incluir información sobre los clientes, pagos y empleados y propiedad intelectual. Los datos operativos críticos pueden incluir registros financieros, características de las cargas, información sobre los procesos de carga de los buques y manifiestos de pasajeros. Las organizaciones marítimas deben saber dónde se encuentran ambos tipos de datos críticos en sus redes y llevar una contabilidad documentada de esos lugares. Por último, deben pensar

en formular una política de privacidad en la que se señale la forma en que recopila, maneja y procesa los datos de sus clientes, socios, proveedores y otros terceros y publicarla en su sitio web.

- **Controlar el acceso a los datos.**

Las organizaciones marítimas deben controlar el acceso a los datos de acuerdo con su sensibilidad. Una vez que se han clasificado los datos, pueden establecer privilegios y derechos de acceso basados en las funciones y responsabilidades. En general, solo deben tener acceso a cierta información las personas que tengan la necesidad explícita de tenerlo. Por ejemplo, aunque los supervisores de operaciones de las terminales podrían requerir el acceso a los datos sobre la carga, no se les debe permitir este acceso a los gerentes de recursos humanos.

- **Proteger los datos.** Además de los controles y procedimientos administrativos que regulan los derechos de acceso, las salvaguardas técnicas también son esenciales para proteger los datos. Dos mecanismos clave para la protección de datos son una combinación de la identificación del usuario y su contraseña y la encriptación. Las organizaciones marítimas deben pensar seriamente en encriptar sus datos administrativos y operativos críticos.

- **Respaldar los datos.** Si los datos de una organización marítima se ven comprometidos, son robados o destruidos o incluso borrados accidentalmente, una copia de respaldo la ayudará a recuperarlos y volver a operar normalmente. Las organizaciones marítimas deben formular una política sobre copias de seguridad en la que se identifiquen los datos que requieren ser respaldados, se defina la frecuencia de los respaldos y se identifique dónde se

almacenarán. Todas las organizaciones marítimas, en especial las que se ubican en regiones geográficas propensas a los desastres naturales, deben considerar el respaldo de sus datos en un centro de datos alejado y seguro.

- **Planear para casos de pérdida de datos.** Las organizaciones marítimas deben contar con planes de contingencia actualizados periódicamente para prever la pérdida inesperada, la interrupción o la destrucción de datos críticos. Los planes de contingencia deben incluir procesos para la notificación de incidentes, el aviso a los clientes, empleados y terceros cuyos datos pudieran haberse visto afectados por una vulneración y la forma en que la organización llevará a cabo operaciones críticas como el manejo de las cargas y el almacenamiento y transporte de combustible en tanto se encuentre temporalmente incapacitada para tener acceso a datos críticos.

### 5.1.2 Políticas sobre tecnología

Además de gestionar una cantidad considerable de datos, las organizaciones marítimas utilizan un número significativo de tecnologías en sus operaciones. Así pues, deben establecer políticas para regir el uso de las tecnologías por parte de su personal. Entre las políticas fundamentales se cuentan:

- **Política sobre uso aceptable.** Las organizaciones marítimas deben establecer una política que defina las prácticas y restricciones con las que los usuarios deben expresar su acuerdo para poder tener acceso a las redes de la organización y al internet en relación con sus activos. Esta política le debe dar al personal la flexibilidad necesaria para que cumpla con las responsabilidades que tiene asignadas a la vez que define las reglas de conducta en línea y establece límites

para proteger a la organización. Con el uso creciente de los dispositivos móviles en las organizaciones marítimas, como teléfonos celulares, tabletas y escáners de identificación por radiofrecuencia, las organizaciones marítimas deben plantearse el establecimiento de una política específica para el uso aceptable de los dispositivos móviles.

- **Política sobre dispositivos personales.**

Algunas organizaciones marítimas, particularmente las pequeñas y medianas, podrían permitir que sus empleados hagan uso de sus dispositivos personales para sus funciones asignadas. Aunque esto le permite a la organización ahorrar en la compra y reemplazo de tecnología, también genera riesgos de seguridad. Las organizaciones marítimas que les permiten a sus empleados utilizar sus dispositivos personales para sus funciones asignadas deben tener una política con respecto a estos dispositivos que establezca los controles de seguridad mínimos requeridos, la propiedad de los datos y los derechos de la organización de modificar el dispositivo y borrar los datos de manera remota.

- **Política sobre medios sociales.** Los medios sociales pueden ser útiles para las organizaciones marítimas que desean promover sus actividades y comunicarse con clientes, socios y proveedores. No obstante, puesto que los atacantes cibernéticos utilizan con frecuencia los medios de comunicación social para obtener información que pueda servir de base para sus actividades de ingeniería social, las organizaciones marítimas deben formular una política sobre los medios sociales que debe incluir pautas sobre las condiciones en que el personal puede revelar información o actividades específicas de la organización en las redes sociales, las normas de comportamiento para el personal que utiliza las redes sociales por motivos personales y directrices sobre el uso de contraseñas únicas para las cuentas de las redes sociales de la organización.





## 5.2 Mejores prácticas operativas

### 5.2.1 Capacitación

Muchas organizaciones han invertido una cantidad considerable de recursos para asegurar la tecnología, pero una cantidad mucho menor para garantizar que el personal utilice la tecnología de forma segura<sup>54</sup>. Sin embargo, los análisis han determinado sistemáticamente que los errores humanos son la razón principal del éxito de los ataques cibernéticos<sup>55</sup>. Los empleados suelen ignorar las medidas de seguridad<sup>56</sup> y muchas organizaciones reconocen que sus empleados son su mayor debilidad en términos cibernéticos<sup>57</sup>. Por estas razones, a menudo las fuentes de los riesgos cibernéticos y los blancos de los ataques cibernéticos son los humanos y no las tecnologías en sí<sup>58</sup>. La capacitación para que el personal sea consciente de los riesgos cibernéticos es una de las medidas más rentables y consecuentes que puede tomar una organización marítima. La capacitación debe ser de dos tipos: de concientización general y a la medida.

#### 5.2.1.1 Capacitación de concientización general

El Instituto SANS, una empresa privada estadounidense dedicada a la seguridad cibernética, descubrió que sin capacitación en seguridad cibernética, el personal de una organización tenía entre un 30% y un 60% más probabilidades de sucumbir a ataques de ingeniería social<sup>59</sup>. Las organizaciones marítimas que capacitan a su personal tienen menos probabilidades de sufrir interrupciones operativas como resultado de un incidente cibernético y cuando se producen esas interrupciones, tienen un menor impacto en la organización. La capacitación de concientización debe cubrir, por lo menos los riesgos relativos a:

- El uso del correo electrónico y el internet.
- La ingeniería social.
- El uso de dispositivos móviles personales.
- La instalación y el mantenimiento del software.
- Las malas prácticas de seguridad del software y de los datos.
- La protección de los datos sensibles.
- La detección de actividades sospechosas.
- La implementación de medidas preventivas de mantenimiento, como parches y actualizaciones.



Adicionalmente, el programa de capacitación general de concientización cibernética de las organizaciones marítimas debe:

- **Requerir capacitación para todo el personal.** Las organizaciones marítimas deben requerir capacitación para todo el personal, incluyendo los altos ejecutivos, los miembros del Directorio, el personal administrativo, los empleados de terminales y otras operaciones, los proveedores que trabajan en el sitio y cualquier otro tercero externo que tenga acceso a los sistemas de tecnologías informáticas y operativas. Debido a la variedad de sistemas de tecnología de la información y operativa que el personal administrativo y de operaciones utiliza como parte de sus funciones, estas organizaciones deben considerar la posibilidad de adaptar esta capacitación de concientización a sus entornos operativos específicos.
- **Utilizar una variedad de técnicas de capacitación.** Las organizaciones marítimas deben recordar que los distintos empleados aprenden de diferentes maneras. Por ende, deben implementar varias técnicas, como sesiones en aulas, sitios web dedicados a la concientización sobre seguridad y consejos útiles por medio de correos electrónicos y carteles. Estas técnicas pueden ayudar al personal a comprender las directrices, políticas, procedimientos y mejores prácticas organizacionales.
- **Asegurar que la capacitación sea recurrente.** Debido a la constante evolución de las amenazas cibernéticas conforme los atacantes diseñan nuevas metodologías, modifican sus herramientas y diseñan tácticas para comprometer las redes seguras, la capacitación para crear conciencia sobre la seguridad cibernética no debe ser una actividad anual que solo se lleve a cabo para marcar una casilla. La capacitación debe ser tanto relevante como recurrente para todo el personal marítimo. Esto ayudará a la organización a establecer y mantener una defensa más sólida contra las amenazas cibernéticas conocidas y nuevas.

#### 5.2.1.2 Capacitación a la medida

Además de la capacitación general de concientización cibernética para todo el personal, es importante que el personal técnico reciba capacitación sobre cibernética adaptada específicamente a las características y el entorno de la organización. Aunque el tipo de capacitación variará según el entorno y las habilidades técnicas de los empleados individuales, las organizaciones marítimas deben buscar asegurarse de que la capacitación comprenda:

- Una consideración especial de los sistemas y redes más importantes de la organización, que deben incluir los sistemas involucrados en operaciones críticas, como la manipulación de las cargas y las tareas administrativas críticas, como el manejo de los datos sensibles de sus clientes.
- Una comprensión de la convergencia entre las tecnologías informáticas y operativas y las complejidades particulares de la organización. Las organizaciones marítimas están integrando cada vez más sus sistemas de tecnologías informáticas y operativas y el personal técnicos debe comprender dónde ocurre esta integración y estar preparado para tomar medidas para mitigar los riesgos cibernéticos relacionados con esta interconexión.

- Actualizaciones para reflejar la evolución del entorno de amenazas cibernéticas relevantes para la organización. Las amenazas cibernéticas evolucionan constantemente. El personal técnico debe estar capacitado en materia de amenazas y vulnerabilidades en función de la inteligencia sobre amenazas y otra información relacionada (véanse las secciones 5.2.6 y 5.2.7).
- Información relevante para los oficiales de seguridad de las instalaciones portuarias y otro personal de seguridad. Los oficiales de seguridad de las instalaciones portuarias y otro personal de seguridad debe recibir capacitación sobre las maneras en que los activos y plataformas de seguridad digital, como los sistemas de televisión de circuito cerrado y de acceso con tarjetas conectados a la red, pueden estar conectados con otros activos de la organización, además de los riesgos que plantean esas conexiones. También deben comprender la necesidad de proteger físicamente las áreas con activos digitales importantes, como las salas de servidores.

## 5.2.2 Manejo del control de acceso ciberfísico

Los atacantes pueden explotar una debilidad en la seguridad de un área de las operaciones de una organización para obtener acceso legítimo a otra área, como ocurrió en el ataque al Puerto de Amberes (véase la sección 2.3.2.1). Debido a este carácter integrado de los riesgos cibernéticos y físicos, es fundamental que las organizaciones marítimas consideren un enfoque también integrado de planeación e implementación de seguridad digitalizada para sus entornos operativos. Las organizaciones marítimas deben evaluar cuidadosamente sus capacidades, procesos y operaciones internas de seguridad para detectar posibles deficiencias y procurar comprender cómo una deficiencia en un entorno operativo podría servir como punto de ingreso y posterior trampolín hacia áreas más sensibles. Las organizaciones deben considerar:

- **Asegurar la segmentación de las redes.** Las mejores prácticas de segmentación de las redes sugieren que los sistemas de tecnologías informáticas y operativas se deben mantener separadas. En ocasiones los beneficios en eficiencia pueden superar esta consideración, pero las organizaciones marítimas deben analizar los riesgos de enlazar los sistemas de seguridad habilitados

para tecnologías de la información con los sistemas críticos habilitados para tecnologías operativas.

- **Invertir en seguridad integrada.** Estas inversiones en seguridad integrada deben estar coordinadas con los requisitos para cumplir las normas, como las que contiene el Código PBIP (véase la siguiente viñeta) y adaptarse a la evolución tecnológica continua de la industria marítima.

- **Actualizar el plan de protección de las instalaciones portuarias existente.** Las organizaciones marítimas sujetas a los requisitos del Código PBIP deben actualizar su plan de protección de las instalaciones portuarias existente si despliegan nuevas capacidades ciberfísicas integradas que conlleven cambios materiales a ese plan.

- **Controlar el acceso a sus activos.** El acceso físico a zonas con activos digitales importantes, como las salas de servidores, permite el acceso lógico a un activo digital. Las organizaciones marítimas deben proteger físicamente las áreas delicadas y restringidas o los bienes tangibles para limitar ese acceso.



### 5.2.3 Seguridad del correo electrónico

El correo electrónico es una herramienta fundamental para las funciones cotidianas de una organización marítima. Aunque el uso del correo electrónico conlleva riesgos, los beneficios superan con creces las posibles consecuencias negativas. No obstante, para proteger los datos, las organizaciones marítimas deben redactar políticas básicas, aplicar las herramientas necesarias e implementar los controles adecuados para apoyar el uso del correo electrónico. Para garantizar un uso adecuado y seguro del correo electrónico, deben:

- **Formular una política de uso del correo electrónico.** Una política eficaz de uso del correo electrónico puede estimular las comunicaciones positivas y productivas a la vez que protegen a la organización de violaciones a la seguridad cibernética. Esta política debe definir claramente los parámetros de uso apropiado y las expectativas para todo el personal, incluyendo recordatorios de que los usuarios deben:

- Desconfiar de los mensajes de remitentes desconocidos.

- Nunca abrir archivos adjuntos de remitentes desconocidos.

- Nunca hacer clic en los enlaces de los correos electrónicos.

- Verificar la autenticidad de las solicitudes de información sensible antes de enviar información de ese tipo.

Esto es especialmente útil para las organizaciones marítimas cuyo personal trabaja en muchos idiomas diferentes, incluidos los que no son sus idiomas nativos.

- **Formular una política de conservación de los correos electrónicos.** Todos los correos electrónicos que se envían desde las direcciones de correo electrónico de la organización deben ser de su propiedad. Con frecuencia, estos correos incluyen información valiosa para y sobre la organización. En consecuencia, las organizaciones marítimas deben considerar cómo gestionan y almacenan los correos electrónicos en los sistemas internos y sus copias de seguridad y recuperación de datos. También deben tener en cuenta los requisitos legales y



normativos, como los relacionados con la privacidad de los datos (que se trataron en la sección 3.4).

- **Implementar medidas anti-spam.**

El correo electrónico se ha convertido en un medio eficaz para desplegar un ataque cibernético, ya que más del 90% de todos los ataques a las redes de empresas son resultado de phishing o spear phishing exitoso<sup>60</sup>. Los filtros de correos electrónicos no deseados son un elemento importante de una estrategia de seguridad del correo electrónico, y las organizaciones marítimas, muchas de las cuales llevan a cabo negocios críticos a través de correo electrónico, deben activar las actualizaciones automáticas de sus aplicaciones, filtros de correos electrónicos y software antivirus. Existen tres medidas antispam específicas cada vez más importantes diseñadas para aumentar la fidelidad y la confianza entre remitentes y destinatarios: el Convenio de Remitentes (SPF), la firma de correos electrónicos (también conocida como DomainKeys Identified Mail, o DKIM), y la autenticación de mensajes, informes y conformidad basada en el dominio (DMARC), que utiliza tanto SPF como DKIM. Como una práctica óptima, los administradores deben configurar al menos SPF y DKIM para mejorar la entrega del correo electrónico y establecer comunicaciones más garantizadas. Aunque su adopción está menos extendida, las organizaciones marítimas que cuentan con SPF y DKIM pueden considerar la implantación de DMARC.

- **Capacitar al personal en el uso seguro del correo electrónico.** La mayor parte del personal de las organizaciones marítimas utiliza el correo electrónico como medio de comunicación para fines empresariales. Estas organizaciones deben capacitar periódicamente a su

personal sobre el uso seguro del correo electrónico y sobre las formas de identificar los posibles riesgos cibernéticos y el uso inadecuado y saber a quién dirigirse en caso de un incidente. Esta capacitación debe estar en consonancia con la política de uso del correo electrónico de la que se habla en esta sección.

#### 5.2.4 Protección contra la ingeniería social

Muchos ataques con correo electrónico consisten en engañar a personas desprevenidas para que se salten los controles de seguridad normales y divulguen información sensible o confidencial o faciliten involuntariamente el acceso a las redes de la organización, un proceso que se conoce como ingeniería social y que puede adoptar muchas formas, como:

- **Phishing** (suplantación de identidad): una forma de comunicación que parece provenir de una fuente legítima o de confianza, pero que en realidad es un engaño diseñado para convencer al destinatario para que haga clic en un hipervínculo contenido en el texto o abra o descargue un archivo adjunto.
- **Spear-phishing:** un tipo de phishing que se personaliza específicamente para el destinatario, normalmente utilizando marcas comerciales específicas o incorporando grupos de afinidad o causas sociales hacia las que muestra lealtad o simpatía.
- **Vulneración del correo electrónico empresarial:** el uso de fraude por correo electrónico para atacar a una organización y lograr resultados específicos que la afectan negativamente.

- **Pretexting:** un ataque de phishing en el que el atacante se hace pasar por un agente de confianza con facultades o responsabilidades percibidas.

- **Whaling:** un tipo de ataque de spear-phishing contra ejecutivos de alto nivel, responsables de decisiones clave, miembros del Directorio o comisarios.

- **Tailgating:** una situación en la que una persona no autorizada sigue a una persona autorizada hacia un lugar seguro, como una zona restringida dentro de una instalación de terminal, para obtener acceso físico a las tecnologías operativas (como grúas, operaciones de carga de mercancías, controles y carga de combustible), sistemas basados en la información (como operaciones de seguridad y sistemas informáticos y seguimiento del tráfico de buques) o bienes protegidos (como almacenes de carga).

- **Vishing:** una combinación de voz y phishing en la que el atacante utiliza el teléfono para acceder a información o sistemas sensibles.

- **Baiting:** dejar dispositivos extraíbles en zonas muy transitadas de una organización o conferencia para que un usuario los introduzca posteriormente en una estación de trabajo e instale malware en el sistema y la red inadvertidamente.

- **Spoofing de correo electrónico:** una falsificación electrónica en la que la dirección de correo electrónico en el campo "De" no es la del remitente real.

- **Water-holing:** una estrategia en la que un atacante adivina u observa qué sitios web utiliza a menudo una organización e infecta uno o varios de ellos con malware.

La ingeniería social se aprovecha del deseo de sus víctimas de confiar o ser útiles y las engaña para que revelen información o permitan el acceso a una red o sistema cuando en otras circunstancias no lo harían. Los ingenieros sociales sacan partido de las tendencias humanas, como devolver favores, sentirse socialmente aceptados u obedecer a la autoridad<sup>61</sup>. Para protegerse contra la ingeniería social, las organizaciones marítimas deben:

- **Capacitar al personal** para que sea consciente de las formas comunes de ataques de ingeniería social y del tipo de información que envía por correo electrónico o proporciona por teléfono y se dé cuenta cuando una comunicación exprese presión o urgencia.

- Tener una **política de notificación de actividades sospechosas** y un mecanismo para esta notificación, como una línea telefónica directa o una dirección de correo electrónico dedicada a la que el personal pueda remitir los correos electrónicos sospechosos de ingeniería social.

- Realizar **pruebas de ingeniería social** para evaluar y revisar la eficacia de la capacitación en ingeniería social.

- Utilizar **software antivirus de buena reputación**.

- Hacer **copias de seguridad periódicas del correo electrónico**.

### 5.2.5 Control de acceso

Las organizaciones marítimas interactúan con una gama diversa de empleados, contratistas, socios y clientes. Para garantizar la confidencialidad,





integridad y disponibilidad de sus datos, deben establecer políticas de control de acceso digital que definan quién puede y quién no puede acceder a determinados activos y datos (véase una descripción del control de acceso ciberfísico en la sección 5.2.2). Estas políticas deben incluir la autenticación, que es la confirmación de que un usuario es quien dice ser, y la autorización, que es el nivel de acceso que se le concede a un usuario. Estas políticas deben considerar:

- **La gestión de la identidad y las contraseñas,** que incluye imponer credenciales de identificación únicas para cada usuario, exigirles a los usuarios que cambien sus contraseñas en el primer inicio de sesión y que posteriormente la cambien con regularidad y mantengan un registro de las contraseñas anteriores para evitar reutilizarlas.
- **Autenticación de dos factores,** que consiste en permitirle el acceso a un usuario sólo después de que ha presentado dos datos combinados, como una contraseña y un código de un solo uso enviado a una aplicación de autenticación (la que se recomienda) o a través de un servicio de mensajes cortos (SMS) a su teléfono móvil.
- **Medidas técnicas,** que incluyen el registro de todas las transacciones, la exigencia del uso de firmas digitales, el filtrado de todo el tráfico saliente para evitar la suplantación de identidad y el enrutamiento de todo el tráfico para los servicios de acceso a internet a través de un número limitado de pasarelas de seguridad controladas.
- **Privilegios diferentes para distintos usuarios,** incluyendo funciones de usuario y privilegios de acceso claramente definidos y limitación de ciertos privilegios para determinados usuarios.



### 5.2.6 Recopilación y análisis de información sobre amenazas cibernéticas

Las organizaciones marítimas deben recopilar y analizar información sobre las amenazas cibernéticas y compartir información sobre las amenazas y los ataques exitosos.

Las organizaciones marítimas pueden ser blancos atractivos para los atacantes cibernéticos debido a la gran cantidad de datos e información que generan, acceden, procesan, almacenan o transmiten. Por lo tanto, es importante que tengan acceso a información sobre las amenazas cibernéticas y sus actores a fin de estar mejor preparadas y preparar a otros para mitigar posibles ataques cibernéticos. La inteligencia sobre amenazas cibernéticas puede incluir información de fuentes abiertas o de medios sociales, inteligencia humana, inteligencia técnica e inteligencia de la deep web y la dark web. Para asegurarse de que recogen y analizan la información sobre las amenazas cibernéticas, las organizaciones marítimas deben considerar:

- **Contratar servicios externos de vigilancia en tiempo real de posibles vulnerabilidades y amenazas.** Las organizaciones marítimas disponen de numerosos servicios comerciales de vigilancia. Estos servicios de vigilancia pueden identificar posibles amenazas cibernéticas en los entornos de las organizaciones marítimas, como nuevos programas de malware y vulnerabilidades de software identificadas recientemente. Esta visibilidad es importante para evitar los ataques cibernéticos antes de que se produzcan.
- **Buscar información sobre amenazas cibernéticas de los proveedores de inteligencia a la que puedan recurrir.** Esta información debe incluir datos en tiempo real sobre las tecnologías informáticas y operativas comunes que

atraen a los actores de las amenazas y posibles recomendaciones para corregirlas, como parches y actualizaciones, para evitar ser blanco de ataques cibernéticos, prevenirlos y minimizar sus efectos en caso de que se produzcan. El Centro de análisis e intercambio de información sobre sistemas de transporte marítimo (MTS-ISAC) (<https://www.mtsisac.org/>) podría ser un mecanismo específico para el sector de las organizaciones marítimas.



### 5.2.7 Intercambio de información

Cuando se produce un incidente cibernético, compartir la información al respecto internamente con el personal de la organización y externamente con socios del sector público y privado puede ayudar a una organización marítima a elevar su nivel de preparación cibernética y anticipar más proactivamente los riesgos cibernéticos y la subsiguiente mitigación de las vulneraciones cibernéticas.

#### Intercambio interno de información

Las organizaciones marítimas deben establecer directrices sobre las formas de comunicar la información sobre las amenazas cibernéticas a todos los miembros de la organización. Estas directrices deben:

- Identificar quién en la organización es responsable de coordinar las actividades de intercambio de información cibernética, incluida la información sobre amenazas y las notificaciones de alerta.
- Documentar los procesos para los protocolos de comunicación.
- Definir protocolos específicos para compartir información sensible, que incluyen la clasificación de los datos y los criterios de alerta y jerarquización.
- Establecer criterios para el intercambio de información para calificar, clasificar y priorizar el análisis y la comunicación de datos específicos, incluida la información sobre el personal o la carga, para compartirlas solo con quienes las necesiten.

#### Intercambio externo de información

Las organizaciones marítimas deben establecer directrices para comunicar la información cibernética a terceros interesados fuera de la organización. Estas directrices deben identificar quién en la organización es responsable de compartir la información cibernética con terceros externos con los que la organización está obligada a compartirla y con aquellos con los que debería o podría querer compartirla. Los terceros externos con los que la organización podría estar obligada a compartir información pueden incluir a los funcionarios gubernamentales del puerto y de otros organismos nacionales, lo que varía según los países. La organización podría decidir compartir información cibernética con otros terceros externos, como el Centro de Análisis e Intercambio de Información sobre Sistemas de Transporte Marítimo, con centros de operaciones de seguridad locales y, en su caso, con los organismos que apoyan la respuesta a los incidentes cibernéticos y las actividades de recuperación dentro de ese país, como los equipos nacionales de respuesta a emergencias informáticas (CERT)<sup>62</sup>. Por último, es importante que las organizaciones marítimas establezcan

protocolos oficiales de intercambio de información, como acuerdos de no divulgación y memorandos de entendimiento, y canales de comunicación seguros con los socios con los que comparten información.

#### 5.2.8 Seguridad de las redes, gestión de la vulnerabilidad y conocimiento de situaciones

La mayoría de las organizaciones marítimas manejan entornos complejos e integrados de tecnologías informáticas y operativas. Sus entornos de tecnología de la información se centran en los servicios y dan soporte a casi todos los aspectos de una organización, incluidos los procesos empresariales internos y las comunicaciones, así como las actividades basadas en tecnologías operativas. Por ende, es importante que tengan en cuenta:

- **La comprensión de las amenazas y vulnerabilidades.** La gestión de la vulnerabilidad y las amenazas consiste tanto en la aplicación de la tecnología como en la participación y la supervisión continuos. Como cualquier organización, las organizaciones marítimas deben utilizar cortafuegos, sistemas de detección de intrusos y sistemas de prevención de intrusos como elementos técnicos fundamentales para proteger sus entornos operativos. También deben llevar a cabo pruebas de penetración para determinar dónde puede haber deficiencias o vulnerabilidades en el perímetro de la organización. Por último, deben considerar la posibilidad de emplear un sistema de gestión de información y eventos de seguridad para tener una visión general eficaz y una capacidad de correlación en tiempo real de los posibles eventos y amenazas que puedan afectar las plataformas.
- **La seguridad de las aplicaciones.** A medida que las organizaciones marítimas



adoptan nuevas aplicaciones y, en particular, aplicaciones móviles, es importante garantizar la seguridad de esas aplicaciones. Esto incluye saber qué datos residen o podrían residir en ellas, establecer un proceso eficaz de ciclo de vida de las aplicaciones y efectuar análisis y pruebas antes y después de utilizarlas.

- **La gestión de parches.** Un parche es la corrección de una vulnerabilidad en un programa o una aplicación. Debido al hecho de que la aplicación de parches se realiza en casi todos los activos y sistemas habilitados digitalmente, el número de parches que una organización necesita implementar puede ser significativo. Por esta razón, las organizaciones marítimas que emplean un gran número de sistemas de tecnologías informáticas y operativas deben implementar un proceso disciplinado para determinar los requisitos de gestión de parches y cerciorarse de que se instalen e implementen los parches necesarios. La gestión de parches debe formar parte de un proceso continuo diseñado para reducir las vulnerabilidades.

- **La seguridad en la nube.** La conectividad en la nube proporciona una plataforma para la automatización<sup>63</sup>, los sistemas operativos compatibles con las plataformas del Internet de las cosas<sup>64</sup>, la planificación colaborativa y el intercambio de información en tiempo real<sup>65</sup>, que pueden producir importantes beneficios en eficiencia operativa. Antes de utilizar cualquier servicio basado en la nube, las organizaciones marítimas deben considerar su apetito de riesgo basado en la nube, asegurarse de que manejan el acceso a los entornos de la nube con medidas de seguridad mejoradas, como la autenticación de dos factores, e incorporar requisitos mínimos de seguridad en los contratos de servicios en la nube.

- **La seguridad de los dispositivos móviles.** El creciente uso de tecnologías móviles en las organizaciones marítimas, como los teléfonos celulares, tabletas y escáners de identificación por radiofrecuencia, les proporciona a los atacantes cibernéticos un punto de entrada adicional a través del cual pueden tener acceso a los activos y sistemas. En consecuencia, la seguridad en los extremos incluye ahora los teléfonos inteligentes, tabletas y otros dispositivos móviles (como los escáners de identificación por radiofrecuencia), además de las computadoras, servidores y sistemas conectados. Para tener en cuenta esta evolución, las organizaciones marítimas deben considerar la posibilidad de implementar software de seguridad para dispositivos móviles, encriptar los datos de los dispositivos móviles y establecer un procedimiento para notificar la pérdida o robo de estos dispositivos. Asimismo, las organizaciones marítimas que permiten el uso de dispositivos personales deben considerar el establecimiento de una política de dispositivos personales (véase la sección 5.1.2), listas blancas de las aplicaciones aprobadas para acceder a los datos de la organización y configuraciones y normas mínimas de seguridad para los dispositivos móviles.

- **El almacenamiento y la prevención de la pérdida de datos.** Dado que la mayoría de las organizaciones marítimas sufrirán ataques cibernéticos exitosos, deben asegurarse de almacenar y respaldar adecuadamente sus datos y de que los sistemas críticos de tecnología informática y operativa puedan restaurarse rápidamente. Los métodos para restaurar los datos podrían incluir respaldar todos los datos críticos, probar los respaldos, garantizar que estos se almacenen en instalaciones remotas (lo que es especialmente importante

para las organizaciones marítimas en regiones propensas a los desastres naturales) y encriptar tanto todos los datos en tránsito como los almacenados. La restauración de los sistemas podría incluir el establecimiento de redundancias para los sistemas críticos, la capacitación del personal en el uso de los sistemas manuales y la realización de ejercicios regulares de los planes de recuperación.

### 5.2.9 Gestión de la cadena de suministro y de terceros

Las organizaciones marítimas son actores clave en el complejo entorno logístico mundial y dependen de sistemas digitalmente habilitados y cada vez más integrados que intercambian datos con un gran número de terceros externos. La integración de esta gran variedad de sistemas significa que los atacantes cibernéticos pueden comprometer los sistemas de los clientes, socios y proveedores para explotar los datos de una organización con fines ilícitos. Esto refuerza la necesidad de que las organizaciones marítimas se aseguren de que sus clientes, proveedores y otros terceros con los que intercambian información tomen las medidas adecuadas para minimizar su vulnerabilidad a los ataques cibernéticos. Para gestionar este riesgo cibernético de la cadena de suministro y de terceros, las organizaciones marítimas deben considerar las siguientes medidas:

- **Comprender los flujos de datos hacia y de terceros.** Las organizaciones marítimas deben saber qué datos transmiten y reciben de qué terceros. En particular, deben identificar los datos sensibles que intercambian con terceros, como los detalles confidenciales de los contratos, la información delicada de seguridad, los datos de la carga y la información del personal (véase la sección 5.1.1).

- **Implementar un programa de gestión de terceros.** Este programa debe incluir la definición de las funciones y responsabilidades del personal que trabaja con terceros, así como una política para la gestión de terceros importantes en la que se detalle la clasificación de los terceros, quién dentro de la organización es responsable de la gestión de cada uno y una categorización por niveles de los controles de seguridad para cada uno. También debe definir preguntas de seguridad y controles de la evaluación de los riesgos para la evaluación de los proveedores de la cadena de suministro.

- **Revisar y actualizar los contratos de adquisiciones.** Estos contratos deben incluir cláusulas que definan las normas y medidas de seguridad cibernética, incluyendo la gobernanza, la seguridad física, la seguridad del personal, la seguridad de la información, los planes de gestión de riesgos, los procesos y procedimientos, el control de calidad y los requisitos de respuesta a las vulneraciones cibernéticas. Las organizaciones marítimas también deben considerar cláusulas (por ejemplo, de indemnización y requisitos de cobertura de responsabilidad cibernética) que reduzcan su riesgo financiero si las prácticas de un proveedor dan lugar a un incidente cibernético.

- **Definir los requisitos de capacitación para los terceros.** Todos los terceros, incluidos los proveedores y contratistas, deben completar la capacitación en materia cibernética antes de llegar a las instalaciones de la organización, en especial si su personal va a tener acceso a un activo crítico habilitado digitalmente o a cualquier activo clave de tecnologías informáticas y operativas conectado a una red.

## 5.3 Preparación de una respuesta a incidentes cibernéticos

En el mundo moderno y digital, es casi una certeza que una organización marítima sufrirá un ataque cibernético que pueda interrumpir o degradar operaciones como la manipulación de la carga, dañar equipos y activos como las grúas y sistemas operativos de terminal y producir daños a la reputación. Debido al potencial de importantes costos tangibles e intangibles, las organizaciones marítimas deben estar preparadas para responder, recuperarse y remediar los ataques cibernéticos. Para crear y mantener esta capacidad, deben considerar la posibilidad de establecer (o actualizar)<sup>66</sup>:

- Un plan de respuesta a incidentes cibernéticos que describa cómo prepararse, detectar y responder a incidentes cibernéticos, que puede incorporarse como complemento al plan de respuesta a incidentes no específico para el ciberespacio existente en la organización.
- Un plan de continuidad de las operaciones, que a menudo incluye un plan de continuidad de las actividades de negocios y analiza cómo la organización puede mantener los servicios durante e inmediatamente después de un incidente.
- Un plan de recuperación de desastres que se centre en la transición de los procesos alternativos de vuelta a los procesos regulares después de que se resuelva un incidente.

### 5.3.1 Crear un plan de respuesta a incidentes

Las organizaciones marítimas deben contar con un plan de respuesta a incidentes cibernéticos. Los planes de respuesta cibernética eficaces ayudan a contener el impacto de un incidente, identificar y analizar el incidente para adoptar las contramedidas necesarias, restaurar las funciones normales del sistema o sistemas afectados y evitar que se repitan ataques similares o idénticos. El plan de respuesta a incidentes cibernéticos debe incluir:

- Organizar un equipo de respuesta a incidentes cibernéticos. El equipo debe incluir personal que pueda restaurar las operaciones del sistema, investigar las razones por las cuales una red se vio comprometida o las causas de algún otro incidente cibernético y tomar medidas correctivas para mitigar el riesgo de que un ataque similar pueda ocurrir de nuevo. Es importante que también incluya

personal operativo, como el que participa en las operaciones de las terminales, que pueda ayudar con la implementación de los planes de contingencia cuando debido a un ataque cibernético se interrumpan los sistemas críticos de tecnología operativa, como las grúas y las tuberías.

- Definir protocolos de comunicación para identificar un incidente. Estos protocolos deben definir los procedimientos para alertar sobre los incidentes y abordarlos, que pueden apoyarse con un servicio de asistencia interna o un sistema de manejo de tickets para que la organización pueda identificar, clasificar y hacer frente rápidamente a los posibles incidentes. También deben tener en cuenta la criticidad de ciertos activos y sistemas, como la manipulación de la carga y el manejo y almacenamiento del combustible, y garantizar que los posibles incidentes que afecten los sistemas críticos se aborden rápidamente.





- Definir líneas de comunicación entre el personal de respuesta y con el público. Estas líneas de comunicación deben incluir la identificación de la persona responsable de tomar decisiones en tiempo real durante las respuestas a incidentes. En cuanto a las comunicaciones externas, el plan debe identificar a los terceros externos con los que la organización está obligada a comunicarse (como los funcionarios gubernamentales a cargo del control del puerto y los equipos nacionales de respuesta) y a los terceros externos a los que debe notificar (como los clientes y la prensa), así como las maneras en que se comunicará con ellos.

- Identificar recursos externos importantes para la respuesta a los incidentes cibernéticos. En la mayoría de las acciones de respuesta a incidentes cibernéticos deben participar recursos externos, como análisis forenses, asesorías legales y especialistas en relaciones públicas. Identificar esos recursos en un plan antes de un incidente le permite a la organización recurrir a ellos lo más rápidamente posible después de que ocurre (véase la sección 5.3.3).

- Requerir pruebas y ejercicios periódicos. Probar y practicar los planes de respuesta a incidentes cibernéticos garantiza que el personal esté familiarizado con las medidas que se adoptarán tras la respuesta a un incidente cibernético y que la organización pueda identificar cualquier deficiencia en las respuestas a estos incidentes antes de que ocurra alguno. Es importante actualizar los planes de respuesta a los incidentes cibernéticos sobre la base de las lecciones aprendidas en los simulacros y prácticas. En el caso de las organizaciones marítimas que deben cumplir el Código PBIP, las pruebas del plan de respuesta a incidentes pueden realizarse como parte de los simulacros y ejercicios que exige el Código.

- Establecer acciones de respuesta y recuperación. Estas acciones deben incluir:

- Una evaluación inicial de la vulneración en la que se identifiquen los activos, sistemas o datos de tecnologías informáticas y operativas afectados, una evaluación de los efectos en la integridad de los datos y una determinación de la persistencia de la amenaza y, en caso de que exista, qué otros activos y sistemas pueden estar en riesgo.

- Actividades de mitigación, incluyendo la limpieza, la recuperación y el restablecimiento de los activos y sistemas afectados, la recuperación y el restablecimiento de los datos mediante la eliminación de las amenazas, la corrección de las vulneraciones del software y el restablecimiento de los servicios operativos tan pronto como sea posible.

- Un análisis posterior al incidente, incluyendo la investigación de sus causas, la determinación del impacto operativo en los activos y sistemas de tecnologías informáticas y operativas afectados, la comprensión de las consecuencias financieras, normativas, legales y de reputación y la elaboración de un conjunto de lecciones aprendidas.

### 5.3.2 Planear la continuidad de las operaciones y la recuperación posteriores a un desastre

Inmediatamente después de un incidente cibernético, es importante tener planes para mantener un nivel mínimamente aceptable de servicios y funciones (continuidad de las operaciones) y posteriormente restablecer los servicios y funciones normales (recuperación de desastres) a la brevedad posible. Los planes de continuidad de las operaciones con frecuencia (pero no siempre) adoptan la forma de un plan de continuidad de las actividades de negocios. Las consideraciones de seguridad cibernética para la continuidad de las operaciones pueden incluir:

- La definición de las autoridades, procesos, procedimientos y recursos necesarios para que la organización se recupere de un incidente cibernético, incluidas las ubicaciones de las operaciones de emergencia, las fuentes de respaldos de los datos y los derechos de administración de las tecnologías informáticas de emergencia.
- La identificación de los requisitos para mantener las operaciones mínimas basadas en las tecnologías informáticas y operativas durante y después de un incidente cibernético.

- La determinación de los activos y sistemas de tecnologías informáticas y operativas que deben tener prioridad para su restauración durante y después de un incidente cibernético.

Los planes de recuperación de desastres se centran en las maneras en que la organización puede volver a operar normalmente lo antes posible tras un incidente cibernético. En los planes de recuperación posterior a un desastre, las organizaciones marítimas deben:

- Entender qué datos tiene la organización, dónde los almacena y qué tan críticos son para sus operaciones.
- Crear un inventario de las prioridades de los activos y sistemas de tecnologías informáticas y operativas.
- Establecer objetivos del tiempo y del punto de recuperación para los sistemas y servicios críticos, como la manipulación de la carga y el almacenamiento y la transferencia de combustible.
- Definir procedimientos para proteger los datos sensibles durante el proceso de recuperación.



### 5.3.3 Desarrollar relaciones con los terceros que ayudarán en la respuesta y recuperación de incidentes

Muy pocas organizaciones pueden responder adecuadamente y recuperarse de un incidente cibernético sin ayuda externa. Como parte de la planeación de su respuesta y recuperación de incidentes cibernéticos, las organizaciones marítimas deben identificar a los terceros externos cuya ayuda podrían necesitar en sus esfuerzos de respuesta y recuperación de incidentes cibernéticos, como:

- **Analistas forenses.** Los expertos especializados en el análisis técnico cibernético pueden ser fundamentales para la investigación y reparación eficaz tras un incidente cibernético. Los proveedores comerciales de estos servicios ofrecen cada vez más acuerdos de retención de cero cuotas que les proporcionan a las organizaciones marítimas un acceso rentable a estos conocimientos.
- **Asesoría jurídica.** Un incidente cibernético puede afectar el cumplimiento de las leyes nacionales y locales, incluidas las de privacidad de los datos (véase la sección 4.4), y tener consecuencias legales, incluida la posible responsabilidad legal. Se debe contar con asesoría jurídica especializada con conocimientos específicos para ayudar en la respuesta a los incidentes cibernéticos.
- **Especialistas en relaciones públicas.** La mayoría de los incidentes cibernéticos afectan a terceros externos. Por lo tanto, los expertos en comunicación y relaciones

públicas pueden ayudar a las organizaciones marítimas a garantizar que su amplia gama de partes interesadas, incluidos los clientes, socios, proveedores, reguladores y el público en general, estén debidamente informados sobre estos incidentes.

- **Seguros.** La transferencia de algunos riesgos cibernéticos a través de un seguro es una herramienta de mitigación de riesgos cada vez más común<sup>67</sup>. Las organizaciones marítimas deben considerar sus escenarios de pérdidas cibernéticas más probables, como la vulneración de la información sensible de los clientes o la interrupción de las operaciones de manipulación de la carga. Al considerar estos escenarios, se deben tomar en cuenta los siguientes puntos:

- ¿Las pólizas actuales cubren los escenarios relacionados con pérdidas?
- Si hay elementos faltantes o excluidos, ¿cuáles son?
- ¿Son explícitas todas las coberturas cibernéticas? ¿Algunas de ellas no están explicitadas?
- ¿Cómo responderían las pólizas existentes a un incidente cibernético?
- ¿Ofrece la aseguradora todas las coberturas adecuadas que requiere la organización?

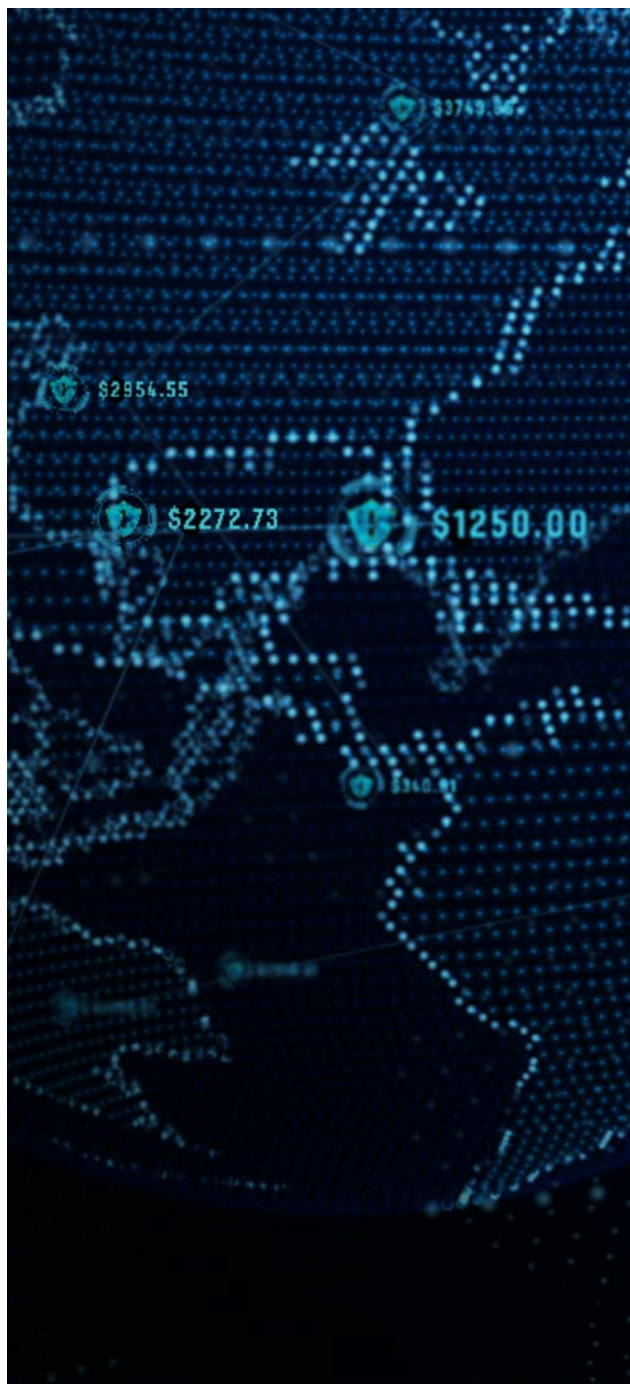


### 5.3.4 Realizar simulacros y prácticas de respuesta a incidentes cibernéticos

Cuando ocurren incidentes cibernéticos, las organizaciones marítimas deben ser capaces de aplicar sus planes de respuesta y continuidad a incidentes cibernéticos y de respuesta a desastres de la forma más rápida y eficaz posible. La capacitación, los simulacros y las prácticas periódicas les permiten implementar estos planes con eficacia e identificar sus deficiencias antes de que se produzca algún incidente.

- **Capacitación.** El personal de las organizaciones marítimas que va a participar en la respuesta a un incidente cibernético debe recibir capacitación en la materia que incluya su comprensión de los procedimientos de recuperación, los métodos para la protección de los datos durante el incidente y el cumplimiento de las metas de tiempo de recuperación. El personal puede provenir de departamentos tan diversos como tecnología de la información, seguridad y operaciones.
- **Simulacros.** Los simulacros de respuesta a incidentes cibernéticos le permiten al equipo de respuesta practicar algunos aspectos del plan de respuesta. También son un mecanismo eficaz para identificar las deficiencias o debilidades técnicas y ofrecen oportunidades para remediarlas.
- **Prácticas.** En las prácticas se detecta si existe conciencia general de los riesgos cibernéticos, se validan los planes y procesos y se evalúan los sistemas y protocolos existentes de respuesta a incidentes y su recuperación posterior. En un ejercicio teórico se simula un incidente cibernético y se les permite a los participantes reunirse para discutir los procedimientos simulados y familiarizarse con diversas situaciones de amenaza posibles. Los escenarios de práctica pueden iniciar con un incidente

cibernético o incluir casos cibernéticos específicos a los que los participantes respondan. Los participantes deben incluir miembros del equipo de respuesta a incidentes cibernéticos de la organización y se debe prestar atención especial a que estén representados los diversos entornos de tecnologías informáticas y operativas de la organización.



# 6.0

## CONCLUSIÓN

El transporte marítimo es crucial para la actividad y el crecimiento económicos mundiales. Es probable que la adopción de tecnologías digitales por parte de la industria marítima continúe, y este aumento de la digitalización y la automatización marítima conlleva el correspondiente aumento del riesgo cibernético marítimo, incluido el hemisferio occidental. Como consecuencia de su creciente complejidad informática y operativa, las organizaciones marítimas son vulnerables a las amenazas cibernéticas por muchas razones, entre ellas el hecho de que manejan una gran cantidad de datos comerciales y, como indican los últimos incidentes, se han convertido en blancos atractivos para los atacantes cibernéticos. Sin embargo, se dispone de poca información sobre el alcance y las consecuencias de estos ataques, ya que los agentes del sector privado suelen ser reacios a poner de manifiesto sus vulnerabilidades públicamente.

Además, la regulación de la gestión de los riesgos cibernéticos está en sus inicios y sigue evolucionando tanto en los organismos internacionales como en las legislaciones nacionales. Aunque las normas vinculantes podrían ser más frecuentes en el futuro, existen reglas, marcos y directrices que pueden servir a las organizaciones marítimas como base de los pasos para organizar, evaluar, gestionar y medir sus riesgos cibernéticos, sus capacidades en materia de seguridad cibernética y su resiliencia cibernética organizacional. Para ello pueden:

- Basar sus estrategias de seguridad cibernética y sus planes de implementación en los marcos y normas existentes para la seguridad cibernética de las infraestructuras críticas.
- Formular documentos clave de gobernanza y políticas para guiar a sus organizaciones y personal en el uso de los sistemas y datos de forma segura.
- Aplicar mejores prácticas operativas para minimizar el riesgo cibernético para sus sistemas y datos.
- Planear la respuesta, la recuperación y la reparación de los ataques cibernéticos cuando se produzcan.
- Compartir información sobre amenazas cibernéticas, vulnerabilidades y ataques a nivel interno y externo.

En el mundo moderno y digital en el que operan las organizaciones marítimas, el riesgo cibernético será un desafío permanente. Sin embargo, se trata de un riesgo que las organizaciones marítimas que adopten un enfoque bien pensado podrán manejar incluso cuando las normas y los marcos internacionales en este ámbito continúen en desarrollo.

# REFERENCES

1. El ámbito marítimo se define como todas las áreas y cosas de, sobre, abajo, relacionadas con, adyacentes a o limítrofes a un mar, océano u otra vía navegable, incluidas todas las actividades que conciernen al mar, la infraestructura, las personas, la carga y los buques y otros medios de transporte
2. Organización Marítima Internacional. 5 de junio de 2020. Carta circular. Coronavirus (covid-19) – Acelerar la digitalización del comercio y la logística marítimos – Un llamado a la acción. Véase: <https://www.wco.int/en/LocalResources/es/MediaCentre/HotTopics/Documents/Circular%20n%C2%BA%204204-Add.20.pdf>
3. En 2004, los Estados Miembros de la OEA subrayaron la importancia de desarrollar una estrategia integral para proteger la infraestructura de la información. En 2015 emitieron una declaración sobre la “Protección de las infraestructuras críticas frente a las amenazas emergentes” y el “Reporte de seguridad cibernética e infraestructura crítica de las Américas”, que destacan cómo los gobiernos de la región tendrán que trabajar con los responsables de las infraestructuras críticas en la protección contra los ataques a sectores cruciales. Véase: <https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf>  
Además, en 2018, la OEA, en colaboración con Microsoft Corporation, publicó un informe en el que se señalan los crecientes esfuerzos de los Estados Miembros de la OEA para abordar las preocupaciones sobre la seguridad cibernética con respecto a su infraestructura crítica. Véase: <https://www.oas.org/es/sms/cicte/cipreport.pdf> (informe disponible solo en inglés)
4. Antes de la pandemia de covid-19.
5. CEPE/ONU. Guía de Implementación de la Facilitación del Comercio. Sistemas de Comunidad Portuaria. Véase: <http://ftg.unece.org/SP/contents/port-community-systems.htm>
6. Más información en <https://csirtamericas.org/>
7. Fintech News. 20 de agosto de 2020. “The 2020 cybersecurity stats you need to know”. Véase: <https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/>
8. The Maritime Executive. 23 de junio de 2020. “Report: Maritime Cyberattacks Have Quadrupled Since February”. Véase: <https://www.maritime-executive.com/article/report-maritime-cyberattacks-have-quadrupled-since-february>
9. Hall, Chris. Wapack Labs, Inc. 14 de junio de 2015. “The Daily Show Agenda”, presentado en la Primera Conferencia de Berlín. Véase: [https://www.first.org/resources/papers/conf2015/first\\_2015\\_-\\_hall\\_-\\_chris\\_-\\_daily\\_show\\_agenda\\_20150618\\_fw.pdf](https://www.first.org/resources/papers/conf2015/first_2015_-_hall_-_chris_-_daily_show_agenda_20150618_fw.pdf)
10. National Infrastructure Advisory Council, Physical/Cyber Convergence Working Group. 16 de enero de 2007. “Final Report and Recommendations by the Council”. Véase: [https://www.dhs.gov/xlibrary/assets/niac/niac\\_physicalcyberreport.pdf](https://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport.pdf)
11. Un ejemplo importante de los ataques cibernéticos con consecuencias físicas fue el ataque Stuxnet. Stuxnet es un gusano informático diseñado originalmente para atacar las instalaciones nucleares de Irán y que desde entonces ha mutado a otras instalaciones industriales y de producción de energía. El blanco original eran los controladores lógicos programables de Siemens que se utilizan para automatizar las centrifugadoras que apoyaban el enriquecimiento de uranio. Se transmitió a través de las redes no conectadas de las instalaciones (conocidas como “air gap”) mediante dispositivos USB y se propagó a través de computadoras con Microsoft Windows. Una vez que el gusano identificaba el equipo objetivo, enviaba órdenes que provocaban daños en el equipo electromecánico y causaban que las centrifugadoras nucleares quedaran fuera de control y se destruyeran. Durante el ataque, el gusano enviaba información falsa al controlador principal, lo que inducía a los ingenieros a tener la sensación de seguridad errónea de que todo estaba bien. Véase: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>
12. Verizon Data Breach Digest. 2015. Véase: <https://www.darkreading.com/operations/pirates-ships-and-a-hacked-cms--inside-verizons-breach-investigations/d/d-id/1324474>
13. Council on Foreign Relations. “Disruption of operations at Shahid Rajaei Port”. Mayo 2020. Véase: <https://www.cfr.org/cyber-operations/disruption-operations-shahid-rajaei-port>
14. Oficina de las Naciones Unidas contra la Droga y el Delito. “Combating Transnational Organized Crime Committed at Sea”. Documento temático. 2013. [https://www.unodc.org/documents/organized-crime/GPTOC/Issue\\_Paper\\_-\\_TOC\\_at\\_Sea.pdf](https://www.unodc.org/documents/organized-crime/GPTOC/Issue_Paper_-_TOC_at_Sea.pdf)
15. Riley, Michael y Jordan Robertson. “The Mob’s IT Department”. BusinessWeek. Julio 2015. Véase: <https://www.bloomberg.com/graphics/2015-mob-technology-consultants-help-drug-traffickers/>





- 16.** Ibid
- 17.** OMI. "Just in Time Arrival Guide". Página xiii. Agosto 2020.  
Véase: <https://www.wcdn.imo.org/localresources/en/OurWork/PartnershipsProjects/Documents/GIA-just-in-time-hires.pdf>
- 18.** United States Cybersecurity and Infrastructure Agency: <https://us-cert.cisa.gov/ncas/alerts/TA17-181A>
- 19.** United Kingdom National Cyber Security Centre: <https://www.ncsc.gov.uk/report/weekly-threat-report-28th-july-2017>
- 20.** Australia Minister for Law Enforcement and Cyber Security: <https://www.dfat.gov.au/sites/default/files/australia-attributes-notpetya-malware-to-russia.pdf>
- 21.** "Global ransomware attack causes turmoil". British Broadcasting Corporation. 28 de junio de 2017.  
Véase: <https://www.bbc.com/news/technology-40416611>
- 22.** Ship Technology. "The ten biggest shipping companies in 2020". 19 de octubre de 2020.  
Véase: <https://www.ship-technology.com/features/the-ten-biggest-shipping-companies-in-2020/>
- 23.** Lloyd's List. "Top 10 box port operators". 1 de diciembre de 2019.  
Véase: <https://lloydslist.maritimeintelligence.informa.com/LL1130163/Top-10-box-port-operators-2019>
- 24.** Osborne, Charlie. "NotPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs". ZDNet. 26 de enero de 2018. <https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/>
- 25.** Morley, Hugh R. "US ports building up cyber attack defenses". Journal of Commerce. 15 de diciembre de 2017.  
Véase: [https://www.joc.com/technology/ports-say-they-take-cyberattacks-seriously\\_20171215.html](https://www.joc.com/technology/ports-say-they-take-cyberattacks-seriously_20171215.html)
- 26.** Intervención en "Securing a Common Future in Cyberspace". Foro Económico Mundial. 24 de enero de 2018.  
Véase: [https://www.youtube.com/watch?v=Tqe3K3D7TnI&feature=emb\\_logo](https://www.youtube.com/watch?v=Tqe3K3D7TnI&feature=emb_logo)
- 27.** Arghire, Ionut. "NotPetya - Destructive Wiper Disguised as Ransomware". Security Week. 29 de junio de 2017.  
Véase: <https://www.securityweek.com/notpetya-destructive-wiper-disguised-ransomware>
- 28.** "Treasury Sanctions Russian Federal Security Service Enablers". Comunicado de prensa. Departamento del Tesoro de Estados Unidos. 11 de junio de 2018. Véase: <https://home.treasury.gov/news/press-releases/sm0410>
- 29.** "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack". Comunicado de prensa. Centro Nacional de Seguridad Cibernética del Reino Unido. 14 de febrero de 2018.  
Véase: <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>
- 30.** Graham, Luke. "NATO-Think-Tank Says a 'State Actor' Was Behind the Massive Ransomware Attack and Could Trigger Military Response". CNBC. 30 de junio de 2017.  
Véase: <https://www.cnn.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html>
- 31.** "Ransomware: Facts, Threats, and Countermeasures". Blog Post. Centro para la Seguridad de Internet (CIS). <https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/>
- 32.** Senzee, Thom. "What Happened in Ransomware Attack on Port of San Diego". San Diego Reader. 10 de abril de 2019.  
Véase: <https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/>
- 33.** "Port of Barcelona Suffers a Cyberattack That Impacted Many of its Servers". Cyware. 24 de septiembre de 2018.  
Véase: <https://cyware.com/news/port-of-barcelona-suffers-a-cyberattack-that-impacted-many-of-its-servers-5f22c204>
- 34.** Mongelluzzo, Bill. "Cosco's Pre-Cyber Attack Efforts Protected Network". 30 de julio de 2018. Journal of Commerce. Véase: [https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network\\_20180730.html](https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html)
- 35.** Osborne, Charlie. "Logistics Giant Toll Group Hit by Ransomware for the Second Time in Three Months". ZDNet. 6 de mayo de 2020.  
Véase: <https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/>

**36.** La OMI es un organismo especializado de la Organización de las Naciones Unidas compuesto por más de 170 Estados que es la autoridad mundial que establece las normas para la seguridad, la protección y el comportamiento ambiental del transporte marítimo

**37.** OMI. Resolución MSC.428(98). Aprobada el 16 de junio de 2017. Véase: <https://www.wcdn.imo.org/localresources/es/OurWork/Security/Documents/Pages%20from%20MSC%2098-23-Add.1%20-%20Anexo%2010.pdf>

**38.** "Directrices sobre la gestión de los riesgos cibernéticos marítimos". OMI. 5 de julio de 2017. Véase: [https://www.wcdn.imo.org/localresources/es/OurWork/Security/Documents/MS-C-FAL.1-Circ.3%20-%20Directrices%20Sobre%20La%20Gesti%C3%B3n%20De%20Los%20Riesgos%20Cibern%C3%A9ticos%20Mar%C3%ADtimos%20\(Secretar%C3%ADa\)%20\(1\).pdf](https://www.wcdn.imo.org/localresources/es/OurWork/Security/Documents/MS-C-FAL.1-Circ.3%20-%20Directrices%20Sobre%20La%20Gesti%C3%B3n%20De%20Los%20Riesgos%20Cibern%C3%A9ticos%20Mar%C3%ADtimos%20(Secretar%C3%ADa)%20(1).pdf)

**39.** El reporte "Seguridad cibernética 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe", Publicaciones (iadb.org), un trabajo conjunto entre la OEA y el BID, proporciona información sobre el nivel de madurez de la seguridad cibernética y una descripción detallada de las capacidades nacionales de los países de América Latina y el Caribe para combatir el ciberterrorismo y garantizar un acceso más seguro al internet en la región. Este estudio analiza la madurez cibernética de cada país en las cinco dimensiones identificadas en el Modelo de Madurez de la Capacidad de Seguridad Cibernética para las Naciones (CMM): (i) Política y estrategia de seguridad cibernética; (ii) Cibercultura y sociedad; (iii) Habilidades de educación, capacitación y seguridad cibernética; (iv) Marcos Legales y Regulatorios; y (v) Normas, organizaciones y tecnologías

**40.** United States Coast Guard Navigation and Vessel Inspection Circular No. 01-20. 26 de febrero de 2020. Véase: [https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC\\_01-20\\_CyberRisk\\_dtd\\_2020-02-26.pdf?ver=2020-03-19-071814-023](https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023)

**41.** United States National Maritime Cybersecurity Plan. Diciembre 2020. Véase: <https://www.whitehouse.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf>

**42.** Directiva (UE) 2016/1148, párrafo 13. 6 de julio de 2016. Véase: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=EN>

**43.** Aunque este documento no pretende abordar los riesgos cibernéticos específicos de las operaciones de los buques, las Directrices de la Conferencia Marítima Internacional y del Báltico sobre seguridad cibernética a bordo de los buques son un recurso útil para aprender más sobre las normas de seguridad cibernética de los buques. Véase: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>

**44.** El NIST CSF se publicó originalmente en 2014 y desde entonces se ha revisado en ocho talleres públicos y con múltiples períodos de comentarios y aportaciones de miles de expertos y representantes de muchos sectores industriales

**45.** Véase una visión general del NIST CSF del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos en [https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework\(CSF\)-ENG.pdf](https://www.oas.org/en/sms/cicte/docs/OAS-AWS-NIST-Cybersecurity-Framework(CSF)-ENG.pdf)

**46.** El informe "Marco NIST: Un abordaje integral de la Seguridad cibernética", publicado por el CICTE/OEA, es un punto de referencia sobre la implementación del Marco NIST en el hemisferio occidental. Véase: <http://www.oas.org/es/ssm/publications.asp?IE=00T78>

**47.** Recursos internacionales del Marco de Seguridad cibernética NIST. Véase: <https://www.nist.gov/cyberframework/international-resources>

**48.** "Latin America steps up data privacy legislative and enforcement efforts". Holland & Knight General Data Review. 7 de mayo de 2019. Véase: <https://www.hklaw.com/-/media/files/insights/publications/2019/04/latinamericastepsupdataprivacylegislativeandenforcementefforts.pdf?la=en>

**49.** Comisión Europea, What Does the General Data Protection Regulation (GDPR) Govern? [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en)

**50.** Parlamento Europeo y Consejo de la Unión Europea (2016) Reglamento (EU) 2016/679, Article 83. Véase: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

**51.** "Risk and Responsibility in a Hyperconnected World". Foro Económico Mundial. Enero 2014. Véase: [http://www3.weforum.org/docs/WEF\\_RiskResponsibility\\_HyperconnectedWorld\\_Report\\_2014.pdf](http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf)

- 52.** Filkins, Barbara. "IT Security Spending Trends". SANS Institute. Febrero 2016.  
Véase: <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>
- 53.** Kulesa, Patrick. "Driving a cyber-savvy culture to combat cyber threats". Willis Towers Watson. 2017. Véase: <https://www.willistowerswatson.com/-/media/WTW/Insights/2017/07/decode-cyber-cyber-savvy-culture.pdf?modified=20170724185825>
- 54.** "The Rising Era of Awareness Training". SANS Institute. 2019.  
Véase: <https://www.knowbe4.com/hubfs/SANS-Security-Awareness-Report-2019.pdf>
- 55.** "Effective Cybersecurity Strategy Rests on People, Not Just Technology". Insurance Journal. 1 de marzo de 2017.  
Véase: <https://www.insurancejournal.com/news/national/2017/03/01/443270.htm>
- 56.** Bhargava, Rishi. "Human Error, We Meet Again". Security Magazine. 6 de diciembre de 2018.  
Véase: <https://www.securitymagazine.com/articles/89664-human-error-we-meet-again>
- 57.** "The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable From Within". Entrada en el blog Kaspersky.  
Véase: <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>
- 58.** Ibid.
- 59.** Lance Spitzner, "Securing the Human". Presentación. SANS Institute. 2013.  
Véase: <https://www.itpss.com/pdf/STH-Presentation-HumanMetrics.pdf>
- 60.** "Improving Your Security Awareness Campaigns: Examples from Behavioral Science". Security Intelligence. Junio 2015.  
Véase: <https://securityintelligence.com/improving-your-security-awareness-campaigns-examples-from-behavioral-science/>
- 61.** Cialdini, Robert. Influence: the Psychology of Persuasion. 1984
- 62.** FIRST es un registro mundial de equipos nacionales de respuesta a emergencias informáticas y equipos de nacionales de respuesta a incidentes cibernéticos a los que el lector puede acudir para identificar sus organismos nacionales. Véase: <https://www.first.org/members/teams/>. Para información específica del hemisferio occidental véase: <https://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/>
- 63.** Olujide, Akintola. "Ports in the Cloud: the Next Step in Automation?" Port Technology. 9 de noviembre de 2018.  
Véase: [https://www.porttechnology.org/news/ports\\_in\\_the\\_cloud\\_the\\_next\\_step\\_in\\_automation/](https://www.porttechnology.org/news/ports_in_the_cloud_the_next_step_in_automation/)
- 64.** "The Internet of Things in Transportation – Port of Hamburg Case Study". SIA Partners. 30 de septiembre de 2016. Véase: <https://www.sia-partners.com/en/news-and-publications/from-our-experts/internet-things-transportation-port-hamburg-case-study>
- 65.** Olujide, Akintola. "Ports in the Cloud: the Next Step in Automation?" Port Technology. 9 noviembre 2018.  
Véase: [https://www.porttechnology.org/news/ports\\_in\\_the\\_cloud\\_the\\_next\\_step\\_in\\_automation/](https://www.porttechnology.org/news/ports_in_the_cloud_the_next_step_in_automation/)
- 66.** Hay una gran variedad de documentos de referencia que pueden utilizar las organizaciones para guiar su formulación de planes de respuesta y recuperación, como la Guía de Manejo de Incidentes de Seguridad Informática del Instituto Nacional de Normas y Tecnología de Estados Unidos (véase: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>) y la Guía de Buenas Prácticas de la Agencia de la Unión Europea para la Gestión de Incidentes (véase: <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>)
- 67.** Abraham, Ben. "New Customised Cyber Insurance Product for Shipowners". Seatrade Maritime News. 28 de abril de 2020.  
Véase: <https://www.seatrade-maritime.com/finance-insurance/new-customised-cyber-insurance-product-shipowners>



LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices

LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices

LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices



LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

**EN EL HEMISFERIO**

# **OCCIDENTAL**

---

Introducción y Directrices



LA SEGURIDAD CIBERNÉTICA

# **MARÍTIMA**

## **EN EL HEMISFERIO**

## **OCCIDENTAL**

---

Introducción y Directrices



**OEA**

Más derechos  
para más gente

ISBN 978-0-8270-7241-1