European Commission

Mecanismo de seguimiento, apoyo y evaluación del programa de rutas marítimas críticas (CRIMSON III)

Ciberseguridad en las infraestructuras marítimas críticas

Reflexión sobre los puertos africanos

Servicio de Instrumentos de Política Exterior

COMISIÓN EUROPEA
Oficina de Cooperación EuropeAid
Instrumento de Estabilidad/ Contrato núm. Nº IFS/2019/410-525

Presentado a:
Ondrej Vosatka
Servicio de Instrumentos de Política Exterior (FPI)
FPI.1 - Paz y estabilidad - Amenazas y desafíos mundiales y transregionales
EEAS 02/9A Rond Point Schuman, Bruselas

Nº de contrato Nº IFS/2019/410-525

Fecha: 20/04/2023

Autores:
Nineta Polemi, Profesora de ciberseguridad, dpolemi@gmail.com
Christophe Van Maele, experto marítimo, cvanmaele@portconsult.eu

Los trabajos fueron coordinados por Evelyn Vancollie, coordinadora del proyecto CRIMSON.

Este estudio está financiado por el Servicio de Instrumentos de Política Exterior (FPI) de la Unión Europea a través del Mecanismo de Seguimiento, Apoyo y Evaluación de las Rutas Marítimas Críticas (CRIMSON III), ejecutado por RUSI Europe. Contó con el apoyo de EU CyberNet.

Este informe se ha elaborado con la ayuda de la UE. El contenido de este informe es responsabilidad exclusiva de los autores y en ningún caso debe considerarse que refleja la opinión de la UE.

Índice

Lista de acrónimos 5

Lista de figuras 7

Resumen ejecutivo 8

1 Introducción 10

2 El complejo ecosistema marítimo 11

3 La Unión Europea (UE) y los puertos africanos 14

3.1 Introducción 14

3.1.1 Puertos africanos 15

3.1.2 Negocio marítimo UE-África 17

4 Conceptos de seguridad marítima 19

4.1 Introducción 19

4.2 Conceptos de seguridad y terminología 19

4.3 Tecnologías marítimas físicas y cibernéticas 20

4.3.1 Digitalización marítima acelerada 22

4.4 Incidentes de seguridad y actores de amenazas 22

4.4.1 Tipos de atacantes 22

4.4.2 Incidentes de seguridad 23

4.4.2.1 Accidentes de seguridad 25

4.4.2.2 Ciberataques 25

4.4.2.3 Ataques de TI/TO 27

4.4.2.4 El uso de ordenadores para comunicarse entre las partes interesadas permite actuar en tiempo real y con eficacia cuando es necesario. Cadena de suministro y amenazas híbridas ... 28

4.4.2.5 Vectores de amenaza 31

5 Normas y estrategias de seguridad marítima 33

5.1 Introducción 33

5.1.1 Estrategia de Seguridad Marítima de la UE (ESMUE) 33

5.1.2 Normas de seguridad marítima 34

5.1.2.1 Código PBIP 34

5.1.2.2 Otros códigos importantes 37

5.1.3 Normas de ciberseguridad 38

5.1.3.1 Normas ISO para la seguridad de las ICI marítimas 38

5.1.3.2 Normas ISA, ANSI para ACS 39

5.1.3.3 Categorización de las normas 39

5.2 Legislación sobre seguridad 41

5.3 Legislación sobre ciberseguridad 42

6 Buenas prácticas de seguridad marítima 44

6.1 Introducción 44

6.2 Gobernanza de la seguridad marítima 44

6.3 Higiene de ciberseguridad de los operadores 45

6.4 Gestión de la seguridad marítima 46

6.4.1 Gestión de la seguridad física 47

6.4.2 Gestión de la ciberseguridad 53

6.5 Ciberresiliencia marítima 56
6.6 Factores humanos 57

7 Prácticas de seguridad portuaria en África 59
7.1 Los puertos del Golfo de Guinea 59
7.2 Organización de la seguridad portuaria en África 59
7.3 Iniciativas internacionales para los puertos africanos 61
7.4 Ciberriesgos en África 62

8 Conclusiones 65

9 Recomendaciones 66
9.1 Recomendaciones para los puertos del África Subsahariana 66
9.2 Recomendaciones a las partes interesadas del sector marítimo africano 67
9.3 Apoyo de la alta dirección 67
9.4 Formación en ciberseguridad 67
9.5 Procedimientos, directrices e instrucciones de ciberseguridad 68
9.6 Servicios y funciones críticos de la organización 68
9.7 Evaluación de los riesgos de ciberseguridad 68
9.8 Plan de gestión de la ciberseguridad 68
9.9 Ciberseguridad de la cadena de suministro 68
9.10 Gestión de incidentes, respuesta y recuperación 68
9.11 Normas y marcos de ciberseguridad 68
9.12 Recomendaciones generales sobre ciberseguridad portuaria 69
9.13 Recomendaciones a la UE: Hacia una colaboración estable UE-África 71

10 Referencias 73

11 Anexos: Cuestionarios de seguridad 76
11.1 Anexo A: Cuestionario de concienciación sobre gobernanza de la seguridad 76
11.2 Anexo B: Cuestionario sobre prácticas de seguridad 80

Lista de acrónimos

AD	Autoridades designadas
AESM	Agencia Europea de Seguridad Marítima
CBP	Código de buenas prácticas
CCTV	Circuito cerrado de televisión
CERP	Control del Estado rector de puerto
CISO	Director de seguridad de la información
Código CIQ	Código internacional para la construcción y el equipo de buques que transporten productos químicos peligrosos a granel
Código IMDG	Código marítimo internacional de mercancías peligrosas
Código IMSBC	Código marítimo internacional de cargas sólidas a granel
COS	Centro de operaciones de seguridad
COSCO	China Ocean Shipping Company
CSA	Evaluación de la ciberseguridad
CSI	Iniciativa para la Seguridad de los Contenedores
CSIRT	Equipo de respuesta a incidentes de seguridad informática
CSO	Responsable de seguridad de la empresa
CSP	Plan de ciberseguridad
CySO	Responsable de ciberseguridad
DDoS	Denegación de servicio (distribuida)
ECDIS / SIVCE	Sistema de información y visualización de cartas electrónicas
EMCIP	Plataforma europea de información sobre siniestros marítimos
ENISA	Agencia de Ciberseguridad de la Unión Europea
EPIP	Evaluación de protección de instalaciones portuarias
EPP	Evaluación de la protección portuaria
ESMUE	Estrategia de Seguridad Marítima de la Unión Europea
GDPR	Reglamento general de protección de datos
GMN	Red mundial MTCC
GNL	Gas natural licuado
IACS	Asociación Internacional de Sociedades de Clasificación
IAPH	Asociación Internacional de Puertos
IA	Inteligencia artificial
IC	Infraestructuras críticas
ICI	Infraestructuras críticas de información
ICS / SCI	Sistema de control industrial
IoT	Internet de las cosas
ISAC	Centro de Análisis e Intercambio de Información
ISM	Gestión internacional de la seguridad
MSC	Compañía Naviera del Mediterráneo
MTCC	Centro de Cooperación en Tecnología Marítima
NIS	Redes y sistemas de información
Nivel de seguridad 1	Nivel de protección PBIP 1, medidas de protección mínimas adecuadas

Nivel de seguridad 2	Nivel de protección PBIP 2, medidas de protección adicionales, mantenidas durante un periodo de tiempo como consecuencia de un mayor riesgo de incidente de protección.
Nivel de seguridad 3	Nivel de protección PBIP 3, se mantendrán medidas de protección específicas adicionales durante un período de tiempo limitado cuando sea probable o inminente un suceso que afecte a la protección marítima
NML	Nuevo marco legislativo
OIT	Organización Internacional del Trabajo
OMI	Organización Marítima Internacional
OPIP	Oficial de protección de instalaciones portuarias
OPP	Oficial de protección del puerto
OSE	Operadores que prestan Servicios Esenciales
PCS	Sistema de comunidad portuaria
PBIP	Protección de los buques y de las instalaciones portuarias
PNT	Procedimientos normalizados de trabajo
PPB	Plan de protección del buque
PPP	Plan de protección del puerto
PSD	Proveedores de servicios digitales
RA	Evaluación de riesgos
RFID	Identificador por radiofrecuencia
RIB	Embarcación neumática rígida
RM	Gestión de riesgos
RMF	Marco de gestión de riesgos
SCADA	Control de supervisión y adquisición de datos
SCSO	Oficial de ciberseguridad del buque
SEAE	Servicio Europeo de Acción Exterior
SGS	Sistema de gestión de la seguridad
SGSI	Sistema de gestión de la seguridad de la información
SIA / AIS	Sistema de identificación automática
SMS	Sistema de gestión de la protección
SMSSM	Sistema Mundial de Socorro y Seguridad Marítimos
SOLAS	Convenio internacional para la seguridad de la vida humana en el mar
SSO	Oficial de seguridad del buque
STCW	Formación, titulación y guardia para la gente de mar
TI	Tecnologías de la información
TIC	Tecnología de la información y la comunicación
TO	Tecnología operativa
TOS	Sistema operativo del terminal
YARIS	Red regional de intercambio de información - Arquitectura de Yaundé

Lista de figuras

Figura 1 : Entorno marítimo 11

Figura 2: Puertos africanos 16

Figura 3 : La protección incluye la seguridad y la ciberseguridad 19

Figura 4: Taxonomía de activos de los puertos marítimos de ENISA 20

Figura 5 : Tecnologías de los buques 21

Figura 6: Tecnologías portuarias 22

Figura 7: Taxonomía propuesta por ENISA para los ataques a la cadena de suministro. 30

Figura 8: Taxonomía de las normas de seguridad marítima 40

Figura 9: Enfoque BIMCO sobre la gestión de la seguridad 47

Figura 10: Matriz de apetito de riesgo 54

Figura 11: Enfoque BIMCO sobre la gestión de la ciberseguridad 55

Figura 12: Arquitectura de seguridad física y cibernética SAURON 56

Figura 13: Resiliencia marítima 56

Figura 14: Objetivos de seguridad de la IET 57

Figura 15: Región marítima del Golfo de Guinea 59

Figura 16: Sistema de control perimetral TO 61

Resumen ejecutivo

Los puertos comerciales modernos son una infraestructura crítica que depende en gran medida de los sistemas de información. La seguridad de un puerto depende, pues, de la integridad de los activos físicos y cibernéticos. A pesar de las pruebas de que los puertos se están convirtiendo en objetivos de los piratas informáticos, cuyos ataques pueden afectar tanto a los activos cibernéticos como a los físicos y paralizar las operaciones, demasiados puertos tienen una ciberseguridad inadecuada. Las amenazas físicas, los incidentes y los accidentes a los activos físicos (por ejemplo, terminales, puertas, edificios) de las infraestructuras marítimas o las amenazas y ataques cibernéticos a los activos cibernéticos (por ejemplo, sistemas de comunidad portuaria, sistemas de navegación) pueden poner en peligro las operaciones marítimas, interrumpir las cadenas de suministro y destruir el comercio y los intercambios internacionales.

Este trabajo de investigación ofrece una evaluación de los conceptos de protección marítima (seguridad y ciberseguridad) disponibles para los puertos, así como de las normas, metodologías, mejores prácticas, herramientas y marcos de gestión de la protección, y analiza los regímenes jurídicos y normativos existentes. Además, el informe presenta las ciberamenazas y ataques a los que se enfrenta el ecosistema marítimo (puertos, buques, compañías marítimas, autoridades, cadenas de suministro marítimas) debido a la rápida digitalización. Las consecuencias y repercusiones de estas amenazas para el operador marítimo, las partes interesadas, las economías y la seguridad nacional pueden ser importantes. Las normas, estrategias e instrumentos jurídicos y políticos en materia de ciberseguridad se presentan en este documento como ejemplos de los esfuerzos realizados para abordar de forma holística los retos de la ciberseguridad marítima. Se presentan metodologías, herramientas y directrices de gestión de riesgos basadas en las normas, con el fin de sensibilizar a los puertos sobre los planteamientos internacionales existentes. El cumplimiento de las normas y las estrategias de seguridad existentes mejora la resiliencia de las operaciones, las cadenas de suministro y el comercio internacionales.

El informe también recoge el nivel de concienciación en materia de seguridad de los puertos del África Subsahariana en comparación con los esfuerzos europeos. Los dos cuestionarios que figuran en los anexos, elaborados por los autores, pueden distribuirse a las partes interesadas del sector marítimo africano para autoevaluar el nivel de gobernanza de la seguridad (anexo A) y su nivel de madurez en materia de concienciación y prácticas (anexo B). Los cuestionarios también pueden utilizarse para mejorar su nivel de preparación en materia de seguridad. Por último, se hacen recomendaciones prácticas a la CE sobre cómo establecer mejores relaciones con los puertos africanos para aumentar sus capacidades en materia de seguridad. El informe sirve para alertar a los ministerios marítimos y a los gobiernos de las cuestiones que deben tenerse en cuenta.

Las recomendaciones del informe pretenden mejorar de forma integral la seguridad en los puertos africanos, incluyendo recomendaciones específicas para la ciberseguridad. A escala nacional, es necesario revisar la legislación en materia de ciberseguridad y animar a los altos

cargos de los puertos a que apoyen una inversión en gobernanza de la seguridad que incluya personal y recursos. Sería necesario formar en ciberseguridad a todas las partes implicadas y formar equipos de ciberseguridad. Se recomienda realizar un inventario de todos los activos críticos, incluidos los ciberactivos, tras lo cual una evaluación de riesgos puede identificar las ciberamenazas, los riesgos y las vulnerabilidades. Basándose en ellos, se puede desarrollar un plan de gestión de la ciberseguridad, que incluya la gestión, respuesta y recuperación de incidentes cibernéticos. Los proveedores de equipos de ciberseguridad pueden tener acceso remoto a los equipos, y su ciberseguridad también debe ser evaluada. Existen normas y conocimientos en materia de ciberseguridad que pueden ayudar a los puertos a crear y mantener su ciberescudo.

También se hacen recomendaciones a la UE sobre cómo potenciar la colaboración UE-África en los ámbitos de la seguridad marítima, la ciberseguridad y la seguridad de las cadenas de suministro. La UE debe tratar de establecer colaboraciones estables entre los ministerios de transporte marítimo, las agencias de seguridad y los centros de análisis e intercambio de información marítima. La UE también debería tratar de colmar las lagunas en materia de cibercapacidades con sus socios africanos, entre otras cosas mediante ejercicios realistas. El apoyo transfronterizo al funcionamiento de Centros de Operaciones de Seguridad marítima que prevean y gestionen eficazmente los ciberataques y los incidentes de seguridad también reforzará la colaboración. También será útil armonizar los esfuerzos de certificación marítima, por ejemplo, mediante auditorías y evaluaciones conjuntas de la seguridad de los equipos marítimos para garantizar la privacidad, la seguridad, la transparencia, la interoperabilidad, la rendición de cuentas, la responsabilidad y el cumplimiento de la legislación y las directrices internacionales en materia de seguridad. Por último, debería haber puntos de referencia regulares mediante la realización de análisis comparativos entre puertos de la UE, de la región del África Subsahariana y puertos de otras regiones del mundo. Esto sería útil para destacar los enfoques de seguridad y ciberseguridad UE-África que han tenido éxito y que pueden reproducirse en otras regiones.

1 Introducción

El sector marítimo sostiene las sociedades y las economías mediante el movimiento de personas y bienes vitales, como la energía (transporte de petróleo y gas) y los alimentos. La economía depende en gran medida de la protección física y la seguridad del transporte marítimo de mercancías y pasajeros. Sin embargo, dado que la actividad marítima depende cada vez más de las tecnologías de la información y la comunicación (TIC) para optimizar sus operaciones (por ejemplo, de la navegación a la propulsión, de la gestión de la carga a las comunicaciones de control del tráfico), la ciberseguridad se ha convertido en un requisito esencial. En los últimos años, las ciberamenazas se han convertido en una amenaza creciente que se extiende por todo el ecosistema marítimo (desde los puertos a las compañías marítimas, pasando por otras infraestructuras críticas interconectadas, como el transporte o las autoridades marítimas). La interrupción o indisponibilidad de las capacidades de las TIC marítimas podría tener consecuencias desastrosas, por lo que cada vez es más necesario garantizar la seguridad física y la ciberseguridad frente a ataques físicos, cibernéticos e híbridos.

En este informe, la palabra protección abarca la protección física, la seguridad y la ciberseguridad y debe tratarse de forma holística, no fragmentada, ya que las infraestructuras marítimas críticas (IC) incluyen tanto activos físicos como cibernéticos.

La seguridad física y cibernética son retos clave a escala nacional e internacional. Los puertos comerciales son infraestructuras críticas (IC) y habilitadores económicos clave, por lo que su seguridad es esencial en el negocio marítimo y una de las mayores ventajas de marketing en la competitiva y creciente era digital marítima internacional.

Los puertos son también nodos indispensables de las cadenas de suministro en las que intervienen numerosas partes interesadas estratégicas, socios comerciales y actividades que interactúan entre sí. La seguridad y la sostenibilidad han surgido también como preocupaciones importantes en las cadenas de suministro de los puertos. Identificar y gestionar las amenazas a la cadena de suministro y sus efectos y riesgos en cascada son retos importantes. Las dificultades se deben en parte a la complejidad inducida por el gran número de actividades, procesos, entidades y activos físicos y cibernéticos relacionados e interdependientes en la cadena de suministro. Las metodologías y herramientas de gestión de riesgos específicas para gestionar los incidentes de seguridad física y cibernética en los puertos y sus cadenas de suministro constituyen importantes retos en materia de seguridad.

2 El complejo ecosistema marítimo

Los puertos comerciales, las compañías marítimas y los buques modernos dependen en gran medida del funcionamiento de sistemas de TIC complejos y dinámicos y de cadenas de suministro marítimo basadas en las TIC, y operan en un entorno marítimo complejo. El entorno marítimo (Figura 1) implica a muchas partes interesadas e infraestructuras que interactúan (autoridades, puertos, compañías marítimas y de seguros, industria naval, bancos, cadenas de suministro, otras infraestructuras críticas), así como activos (físicos y cibernéticos).

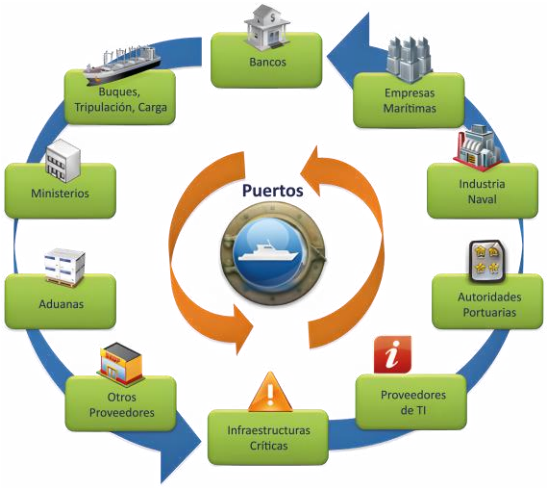


Figura 1: Entorno marítimo[1]

Las infraestructuras marítimas se consideran críticas según las Directivas NIS y NIS2 (Directivas sobre la seguridad de las redes y los sistemas de información)[2] ya que la interrupción de sus operaciones y servicios tendría un impacto negativo en el comercio nacional, comunitario e internacional en general, así como, ocasionalmente, en vidas humanas.

Como Infraestructuras Críticas, las infraestructuras marítimas están obligadas a mantener la seguridad (física y cibernética) de todos sus activos de sus TIC, alojados y operados en sus IC para prestar servicios portuarios. Las TIC marítimas pueden considerarse un cibersistema físico con las seis capas siguientes:

1. Capa de infraestructura (por ejemplo, edificios, plataformas, puertas, puertos deportivos, centros de datos, terminales, barcos)

2. Capa de telecomunicaciones (por ejemplo, redes, equipos de telecomunicaciones, satélites, estaciones repetidoras, estaciones tributarias);

[1] (Polemi, 2017)
[2] (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016); (Negreiro, 2022)

3. Capa de TI (por ejemplo, sistemas de navegación / transmisión / supervisión / comunidad portuaria, SIG, sistemas de vigilancia inteligentes, Internet de las Cosas (IoT));

4. Datos (por ejemplo, datos marinos y costeros, datos comerciales);

5. Servicios marítimos (por ejemplo, facturación, navegación, gestión de equipajes / cargas / buques / contenedores, logística, servicios de la cadena de suministro);

6. Usuarios: a. usuarios internos (por ejemplo, operadores, administradores, tripulación); b. usuarios externos (por ejemplo, autoridades portuarias, compañías marítimas, aduanas, compañías de seguros, proveedores de TI y de la cadena de suministro); y c. objetos inteligentes (por ejemplo, contenedores, buques, carga de tripulación, equipaje, vehículos).

La primera (infraestructura) y la sexta (usuarios) son las capas físicas de las IC marítimas, mientras que las capas 2-5 son las capas cibernéticas. Las partes interesadas del sector marítimo deben garantizar las dimensiones de confidencialidad, integridad y autenticidad de todas las TIC, es decir, la protección de los activos físicos (seguridad) y la protección de los activos cibernéticos (ciberseguridad).

Las IC marítimas tienen una importancia económica creciente y se han convertido en objetivo de los piratas informáticos, que cada vez lanzan más ataques físicos y cibernéticos contra los sistemas de navegación global y los sistemas de gestión de la carga de los puertos y los buques. Estos ataques pueden inutilizar un buque, secuestrar, desviar o robar la carga, además de poner en peligro datos confidenciales de clientes o empresas.

Del mismo modo, los ataques en los sistemas operativos de las terminales portuarias (TOS), los sistemas de comunidad portuarios (PCS) (por ejemplo, control de supervisión, SCADA, sistemas de control distribuido y controladores lógicos programables), o los sistemas de navegación de los buques pueden causar interrupciones o daños en dispositivos mecánicos críticos (por ejemplo, grúas de contenedores, sistemas de seguridad y mecánicos que operan esclusas y presas), y lo que es peor, pueden causar la pérdida de vidas humanas, robar la carga o destruir un buque. Un ataque a un TOS de contenedores también podría interrumpir los servicios intermodales de contenedores que implican transporte marítimo, ferroviario y por camión.

Los TOS portuarios heredados más antiguos tienen una larga vida útil y suelen funcionar en modos independientes con políticas de contraseñas y administración de la seguridad inadecuadas, sin mecanismos ni protocolos de protección de datos que son propensos al fisgoneo, la interrupción y la interceptación, lo que puede causar la perturbación de diversas operaciones y servicios críticos de los puertos y las cadenas de suministro. Los PCS son plataformas electrónicas complejas que conectan múltiples sistemas operados por diversas organizaciones del ecosistema marítimo y una plétora de proveedores de TIC; la seguridad de los PCS se trata como una "caja negra" criptográfica, donde el funcionamiento interno está

oculto y sólo se conocen las entradas y salidas.[3] Las Ventanillas Únicas Nacionales, que se basan en el PCS, deben ser evaluadas y las políticas de seguridad que las acompañan deben garantizar su funcionamiento fiable.

Por desgracia, la mayoría de las partes interesadas del sector marítimo utilizan prácticas de gestión de la seguridad no normalizadas ni armonizadas, que se centran en las amenazas y los puntos débiles físicos, ignorando los cibernéticos. Tanto los incidentes físicos como los de ciberseguridad pueden poner en peligro el funcionamiento de los puertos, los buques y toda la cadena de suministro, causando trastornos económicos, perturbaciones en los sistemas de transporte y en el comercio internacional. Además, la interrupción de las cadenas de suministro puede convertirse en un objetivo para los terroristas internacionales si los puertos y todas las entidades de la cadena no han realizado los controles de seguridad adecuados.

Este informe sirve como manual de concienciación y Guía de Buenas Prácticas que explica los principales problemas de la protección (seguridad y ciberseguridad) de las Infraestructuras Críticas de Información (ICI) marítimas, las ciberamenazas y los ataques a los que se enfrenta el ecosistema marítimo (puertos, buques, compañías marítimas, cadenas de suministro marítimas) debido a la rápida digitalización. Las consecuencias y repercusiones de estas amenazas para el operador marítimo, las partes interesadas, las economías y la seguridad nacional pueden ser inmensas. Se presentan normas, estrategias e instrumentos jurídicos y políticos en materia de ciberseguridad que sirven de ejemplo de los esfuerzos realizados para abordar de forma holística los retos de la ciberseguridad marítima. Se presentan metodologías, herramientas y directrices de gestión de riesgos basadas en las normas para sensibilizar a los puertos africanos sobre los enfoques internacionales existentes. El cumplimiento de las normas y las estrategias de seguridad existentes mejora la resiliencia y la colaboración, lo que puede garantizar la seguridad de las operaciones, las cadenas de suministro y el comercio internacionales. Por último, se ofrecen recomendaciones para los puertos africanos y cuestionarios para captar la madurez de los puertos en materia de ciberseguridad.

[3] (Acharya, 2019)

3 La Unión Europea (UE) y los puertos africanos

3.1 Introducción

Definiciones clave:

Instalación portuaria: lugar donde se realiza la interfaz buque-puerto. Incluye, según sea necesario, zonas como los fondeaderos, atracaderos de espera y accesos desde el mar [Reglamento (CE) nº 725/2004].

Puerto: cualquier zona especificada de tierra y agua, con límites definidos por el Estado miembro en el que esté situado el puerto, dotada de unas obras y equipo que faciliten las operaciones de transporte marítimo comercial [Directiva 2005/65/CE].

Las IC portuarias incluyen las instalaciones portuarias (activos físicos de los puertos), los activos cibernéticos y los usuarios. Según Alderton (1999), existen 3 tipos clásicos de propiedad y explotación portuaria, a saber *Landlord port* (puerto propietario), *Tool port* (puerto herramienta) y *Service port* (puerto de servicio).

Responsabilidades de la autoridad portuaria (Fuente: Alderton, 1999)[4]			
Tipo de puerto	Infraestructura	Superestructura	Estiba y desestiba
Landlord port	Sí	No	No
Tool port	Sí	Sí	No
Service port	Sí	Sí	Sí

El *Landlord port* es aquel en el que el Estado, la autoridad portuaria o el ayuntamiento son propietarios del terreno y arriendan la terminal a estibadores privados. El Estado proporciona la infraestructura, como muelles y terrenos para la terminal, mientras que el operador privado aporta la superestructura y el equipamiento, como grúas, almacenes, equipos de terminal y otras instalaciones comerciales. Un ejemplo es la Autoridad Portuaria de Rotterdam, que arrienda la infraestructura portuaria al European Combined Terminal (ECT).

El *Tool port* es cuando el Estado es propietario tanto de la infraestructura como de la superestructura, y la empresa estibadora privada proporciona la mano de obra para la explotación. La competencia es muy alta, y las licitaciones se hacen con derechos seguros. Algunos ejemplos son Houston, en Estados Unidos, y la mayoría de los puertos autónomos de Francia.

El *Service port* también se conoce como puerto integral o público. El Estado o la autoridad portuaria son propietarios tanto de la infraestructura como de la superestructura y proporcionan todos los servicios e instalaciones para los buques. Algunos ejemplos son la Autoridad Portuaria de Singapur, que pasó a ser privada en 1997, y los puertos de India, Israel, Sudáfrica y Ghana.

La *capa física de los puertos* incluye muelles, embarcaderos, canales de acceso, etc. En general, las condiciones varían de una terminal a otra dentro de un mismo puerto. Sin

[4] (Alderton, 1999)

embargo, todos los puertos se enfrentan al reto de mantener sus infraestructuras en entornos marinos difíciles.

Superestructura portuaria: las disposiciones de superficie (por ejemplo, para almacenamiento), los equipos fijos (como almacenes y edificios de terminales), así como los equipos móviles (como grúas) situados en un puerto para la prestación de servicios portuarios relacionados con el transporte.

Estiba portuaria: Incluye la carga y descarga y estiba de mercancías en cualquier forma a bordo de los buques en los puertos.

Toda entidad que tenga responsabilidades de Autoridad Portuaria debe identificar sus activos críticos en el ámbito de su responsabilidad y, en consecuencia, evaluar el nivel de riesgo.

Casi todos los activos están vinculados al ciberespacio de tres formas, a saber: 1) el emplazamiento tecnológico y los sistemas de información de comunicaciones (hardware/software); 2) los procedimientos operativos de la tecnología y los sistemas de información de comunicaciones; y 3) las personas y los objetos inteligentes (por ejemplo, IoT) que interactúan con la tecnología y los sistemas de información de comunicaciones.

3.1.1 Puertos africanos

Las exportaciones africanas de bienes y servicios han experimentado su mayor crecimiento en la última década, pero los volúmenes africanos siguen siendo bajos, apenas un tres por ciento del comercio mundial, según el Banco Mundial[5]. El limitado papel de África en el comercio mundial se refleja en los contornos de sus puertos marítimos, que se enfrentan a retos evolutivos en materia de protección, seguridad y ciberseguridad. No obstante, los puertos marítimos son una parte vital de la cadena de suministro en África, ya que el transporte marítimo es la principal puerta de entrada al mercado mundial y cada puerto tiene una extensa zona de influencia que a menudo abarca varios países sin litoral, que constituyen un tercio de África. Por lo tanto, es vital invertir y modernizar los puertos y sus infraestructuras de transporte conexas para hacer avanzar la economía nacional y promover el desarrollo y el crecimiento económico general de África.

Un estudio de PricewaterhouseCoopers (PWC)[6] muestra que los volúmenes económicos que se manejan en los principales puertos del África Subsahariana corresponden principalmente a puertos situados en África Occidental y el Golfo de Guinea (véase la imagen inferior).

[5] (Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book, 2022)
[6] (Strenghtening Africa's gateways to trade, 2018)

Figura 2: Puertos africanos[7]

Los países del Golfo de Guinea dependen de unos mares protegidos y seguros para su desarrollo económico, el libre comercio, el transporte marítimo y la preservación del medio marino. Es una gran región marítima que abarca 18 países con 500 millones de habitantes y se extiende desde Senegal hasta Angola con más de 5.700 km de costa. La región es una importante ruta marítima internacional y representa el 25% del tráfico marítimo africano. El petróleo y el pescado, entre otros muchos tipos de recursos naturales, son mercancías importantes que se transportan a otros países africanos y también a Europa y otros países del mundo en buques comerciales.

Los puertos marítimos son la interfaz entre el mar abierto y el interior. Forman infraestructuras marítimas de importancia estratégica por las que deben pasar todos los bienes económicos. Esto las hace muy vulnerables a los ataques de organizaciones delictivas o grupos terroristas. Los atentados terroristas contra puertos podrían afectar gravemente a las poblaciones locales, a las propias infraestructuras portuarias y a las economías locales y regionales dependientes de estas actividades portuarias.

La UE sigue siendo el principal socio comercial de África, aunque su cuota de comercio ha disminuido, mientras que el comercio con China ha aumentado. Dentro del continente africano, África Occidental es el mayor socio comercial de la UE en el África Subsahariana. Europa importa de África Occidental productos acabados (pescado y textiles), pero también materias primas como combustible y productos agroalimentarios. África Occidental, por su parte, importa de la UE combustibles refinados, productos alimentarios, maquinaria, productos químicos y farmacéuticos. África Occidental es también el destino más importante de las inversiones de la UE en África, según la UNCTAD.[8]

Corresponde a cada país decidir en qué medida se aplican y gestionan adecuadamente sus leyes nacionales de seguridad y el Código internacional para la protección de los buques y de

[7] *(Strengthening Africa's Gateway to Trade*, 2018)
[8] (Maritime trade and Africa, 2018)

las instalaciones portuarias (PBIP) de la Organización Marítima Internacional (OMI). Existe la oportunidad de acompañar a los puertos en una perspectiva amplia para aumentar su resiliencia en materia de seguridad. Este estudio servirá de manual con recomendaciones para mejorar la protección portuaria en el África Subsahariana.

3.1.2 Negocio marítimo UE-África

La importancia del sector marítimo para los Estados miembros europeos y sus economías queda claramente ilustrada por el hecho de que existen 329 puertos comerciales europeos por los que transitan el 74% de las mercancías importadas y exportadas y el 37% de los intercambios dentro de la Unión.

La UE y los EE.UU. son los principales socios comerciales de la región africana.[9] El Global Gateway Africa - Europe Investment Package[10] tiene como objetivo apoyar a África en:

- Acelerar la transición ecológica
- Acelerar la transición digital
- Acelerar el crecimiento sostenible y la creación de empleo digno
- Reforzar los sistemas sanitarios
- Mejorar la educación y la formación

El Centro Africano de Cooperación Tecnológica Marítima (MTCC) se puso en marcha en Mombasa en 2017. Forma parte de la Red Mundial de MTCC (GMN) financiada por la Unión Europea[11]. El MTCC para África (MTCC África) está organizado por la Universidad Jomo Kenyatta de Agricultura y Tecnología (JKUAT), Campus Mombasa CBD, en colaboración con la Autoridad Marítima de Kenia (KMA) y la Autoridad Portuaria de Kenia (KPA).

MTCC África se centra en lo siguiente:

- Facilitar el cumplimiento del Convenio internacional para prevenir la contaminación por los buques (Anexo VI de MARPOL);
- Mejorar la capacidad en la región colaborando con las administraciones marítimas, las autoridades portuarias, los departamentos gubernamentales y las partes interesadas del transporte marítimo para facilitar el cumplimiento de la normativa internacional sobre eficiencia energética de los buques;
- Fomentar la adopción de tecnologías y operaciones con bajas emisiones de carbono en el sector marítimo a través de proyectos piloto;
- Sensibilizar sobre las políticas, estrategias y medidas de reducción de los gases de efecto invernadero y otras emisiones del sector del transporte marítimo;
- Demostrar un sistema a escala piloto de recogida de datos e información sobre el consumo de combustible de los buques para mejorar los conocimientos de los armadores y las administraciones marítimas al respecto;
- Difundir y compartir los resultados y experiencias del proyecto mediante acciones adecuadas de comunicación y visibilidad.

[9] (Coulibaly, Kassa, & Zeufack, 2022)
[10] (EU-Africa: Global Gateway Investment Package, n.d.)
[11] (Africa Maritime Technology Cooperation Centre launched in Mombasa, 2017); (MTCC Africa, n.d.)

- Desarrollar y aplicar estrategias para mantener el impacto de los resultados y actividades del MTCC más allá del plazo del proyecto.

Eurostat declaró en 2021 que el mayor socio comercial de África es Europa, a la que exporta el 33% de sus productos e importa el 31%. Esto equivale a importaciones por valor de 142.000 millones de euros y exportaciones por valor de 146.000 millones de euros de mercancías desde/hacia África en 2021.

África depende en gran medida de buques y puertos para atender su comercio intercontinental, mientras que un tercio de los países sin litoral reciben sus mercancías a través de países con acceso marítimo. Esto significa que el transporte marítimo sigue siendo la principal puerta de entrada a Europa.

El comercio marítimo de África se define por la concentración del comercio internacional del continente en los puertos marítimos. La UNCTAD menciona que los puertos africanos sólo representan el cuatro por ciento del volumen mundial de comercio en contenedores, gran parte del cual comprende importaciones de productos manufacturados. Los puertos africanos no se ajustan a las tendencias mundiales de ratios de contenerización y podrían mejorar sus volúmenes de tráfico portuario en contenedores y aumentar las mercancías de exportación en contenedores. Si se transportara más carga por carretera desde el interior a los puertos, entrarían en ellos más buques portacontenedores, lo que atraería un mayor tráfico internacional.

Para lograrlo, los puertos y las redes de transporte interior de África deben modernizar sus infraestructuras y servicios portuarios, mejorar su rendimiento, aumentar sus niveles de productividad, pero también incrementar sus iniciativas en materia de protección, seguridad portuaria PBIP y ciberseguridad.

4 Conceptos de seguridad marítima

4.1 Introducción

En nuestro mundo preocupado por la seguridad, es difícil recordar una época en la que la seguridad no fuera una prioridad. En la actualidad, las actuaciones en materia de seguridad marítima mejoran cada año en diversas zonas del mundo, con la consiguiente disminución gradual de accidentes, lesiones y ataques físicos y cibernéticos. Pero este tipo de protección no siempre ha sido una prioridad para los armadores y los puertos marítimos. El paso de la reparación a la prevención se ha visto impulsado por accidentes y ciberataques ocurridos en el pasado a bordo de buques, en puertos marítimos y en empresas marítimas. El hilo conductor de estos incidentes fue que las normas de protección (seguridad y ciberseguridad) existentes no se siguieron al pie de la letra y no se aplicaron correctamente en la práctica.

4.2 Conceptos de seguridad y terminología

La literatura internacional utiliza indistintamente los términos seguridad, protección, ciberseguridad, seguridad física y resiliencia.

En este informe, como ya se ha mencionado, las IC marítimas se consideran sistemas físico-cibernéticos con capas físicas y cibernéticas. Las partes interesadas del sector marítimo deben garantizar la seguridad de los activos físicos (seguridad) y la seguridad de los activos cibernéticos dentro de las capas (ciberseguridad). El objetivo de la seguridad marítima es proteger los activos físicos (por ejemplo, buques, edificios, puertos deportivos, centros de datos, carga) y a las personas (por ejemplo, personal, operadores, tripulación) contra diversos tipos de amenazas físicas, por ejemplo, incidentes intencionados y no intencionados, peligros y daños como desastres físicos, tormentas en el mar, incendios, terrorismo, disturbios sociales, contrabando de armas y drogas, piratería. El objetivo de la ciberseguridad marítima es garantizar la confidencialidad, integridad y disponibilidad de todos los activos cibernéticos (por ejemplo, telecomunicaciones, TIC, datos, servicios) frente a las amenazas cibernéticas (por ejemplo, phishing, spoofing, ingeniería social (actividades maliciosas que utilizan interacciones humanas), suplantación de identidades, acceso no autorizado, ataques distribuidos de denegación de servicio (DDoS)).

La seguridad incluye tanto la seguridad como la ciberseguridad, como indica la figura 3.

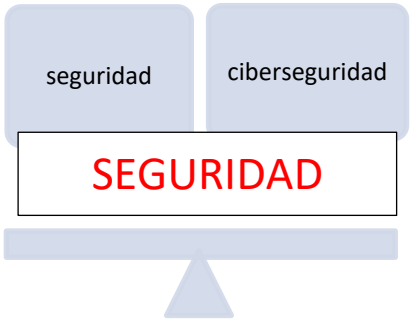


Figura 3: La seguridad incluye la protección y la ciberseguridad

Los activos físicos y cibernéticos pueden estar expuestos a amenazas si no se han implementado los controles/medidas y acciones de mitigación apropiados, dejando los activos vulnerables a amenazas y explotación. En caso de que se produzca un desafortunado incidente de seguridad, se activan los procedimientos de seguridad de emergencia y los planes de recuperación ante desastres y continuidad de la actividad, y se adoptan medidas para mitigar los riesgos. Cuando se produce un incidente, se ponen en marcha una serie de medidas a escala nacional, en consonancia con los planes de emergencia a bordo del buque (Planes de Protección del Buque), en el puerto marítimo (Plan de Protección del Puerto) y en las instalaciones portuarias (Planes de Protección de las Instalaciones Portuarias).

El hilo conductor entre la seguridad y la ciberseguridad es el escudo de protección aplicable en cada ámbito. La construcción de este nivel de protección se lleva a cabo mediante una gobernanza eficaz, tratando de eliminar los riesgos físicos y cibernéticos, evitar los incidentes de seguridad portuaria y prevenir los accidentes humanos. Uno repercute en el otro, por ejemplo, si un ataque de ciberseguridad en una instalación portuaria de carga general detiene repentinamente la operación de manipulación de la grúa, esto podría hacer que la carga cayera en la bodega del buque y podría causar una lesión mortal a los estibadores que se encuentran debajo. Por lo tanto, este estudio aborda **la protección como la combinación de la seguridad y la ciberseguridad** y presenta cómo pueden combinarse los reglamentos, las normas y las mejores prácticas para abordar ambos componentes de la seguridad.

4.3 Tecnologías marítimas físicas y cibernéticas

Los puertos y los buques albergan complejas ICI con activos físicos y cibernéticos utilizados para llevar a cabo sus operaciones y prestar sus servicios marítimos.

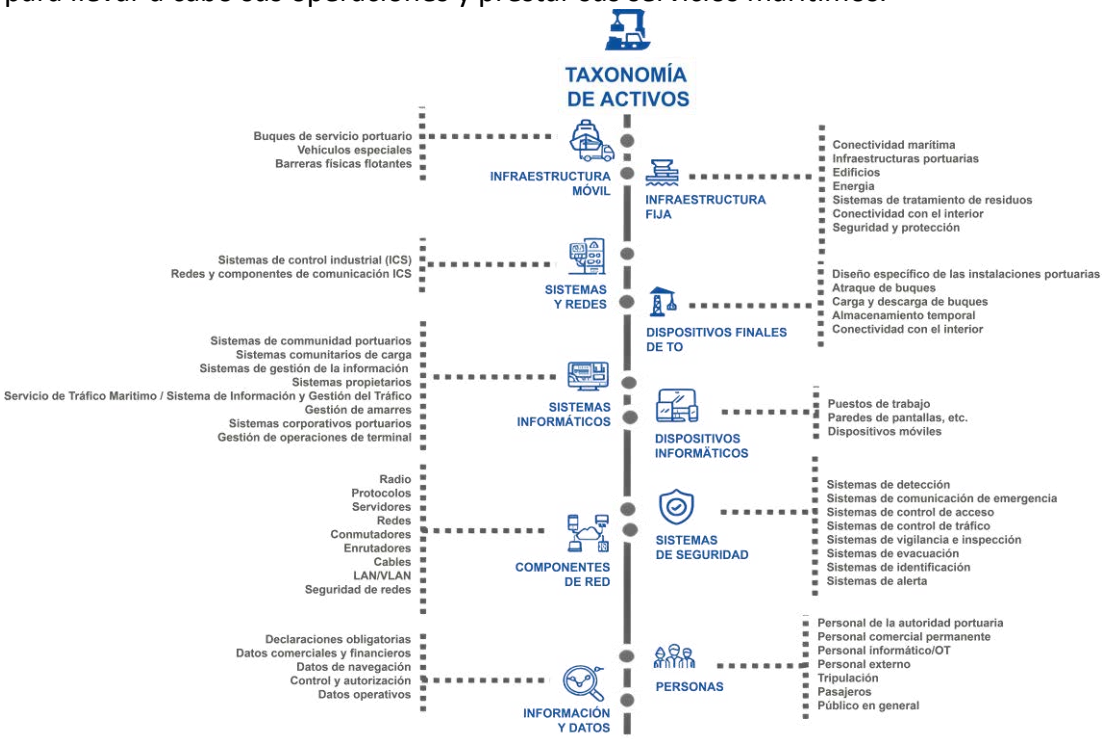


Figura 4: Taxonomía de activos de los puertos marítimos de ENISA[12]

[12] (Drougkas, Sarri, Kyranoudi, & Zisi, 2019)

Los buques están armados con diversas tecnologías, incluyendo: Sistemas de posicionamiento, Sistema de Información y Visualización de Cartas Electrónicas (ECDIS), Sistemas de control y supervisión de motores, Sistema Mundial de Socorro y Seguridad Marítimos (SMSSM), Sistema de Identificación Automática (SIA), SCADA marítimo ICS. La siguiente figura ilustra las tecnologías a bordo:

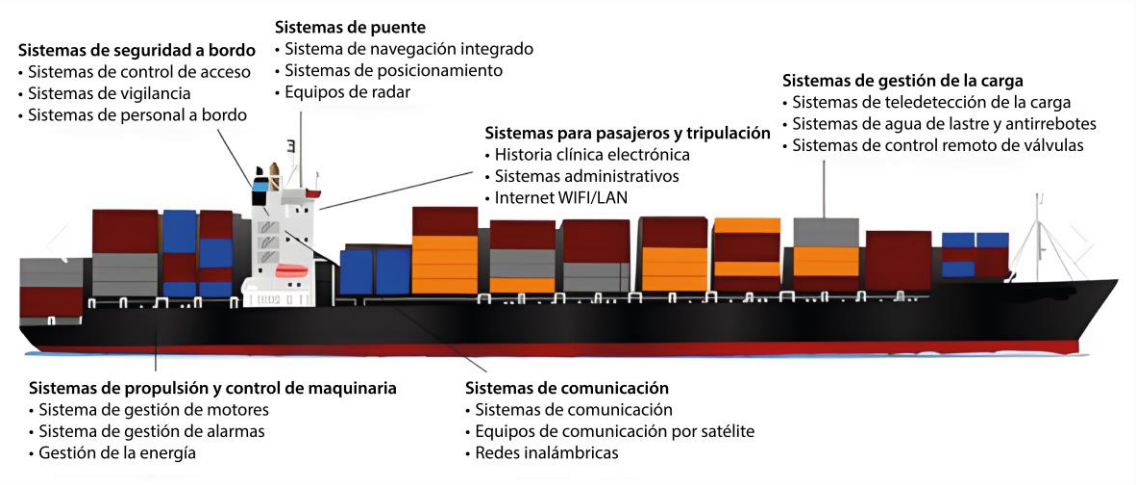


Figura 5 : Tecnologías navales[13]

Las tecnologías portuarias y navales se utilizan para prestar servicios portuarios y de la cadena de suministro marítima, por ejemplo:

- Servicios de atraque de buques
- Servicios de carga y descarga de buques
- Almacenamiento temporal y servicios de estancia
- Servicios de distribución y transferencia
- Servicios de apoyo
- Servicios a las autoridades
- Servicios de seguridad
- Transporte de mercancías (por ejemplo, gas natural licuado (GNL), vehículos, grano)
- Servicios de crucero y transporte de personas
- Servicios de gestión de contenedores
- Servicios de cabotaje

[13] Fuente: https://www.hvassallo.com/practice-areas/maritime-cyber-security/; consultado el 17 de diciembre de 2022

Figura 6: Tecnologías portuarias[14]

4.3.1 Digitalización marítima acelerada

La adopción de tecnologías emergentes, como la Inteligencia Artificial (IA), 5G, Big Data, IoT, robótica y tecnologías satelitales, se está utilizando para nuevos avances marítimos, por ejemplo, buques autónomos, inspección rápida de IC portuarias, incluidas instalaciones de energía eólica, estaciones bentónicas submarinas, automatización de operaciones de prospección sísmica geofísica y geotécnica, supervisión y gestión de buques.

La adopción acelerada de las tecnologías digitales en el ecosistema marítimo dará lugar a numerosas innovaciones en diversas funciones marítimas, por ejemplo, el intercambio de cantidades masivas de información mediante redes avanzadas de comunicación acústica y óptica, la automatización colectiva de las decisiones, la puesta en común de recursos complementarios, la automatización del mantenimiento y las operaciones de puertos y buques. Sin embargo, estas próximas innovaciones irán acompañadas de nuevas amenazas físicas y cibernéticas. La gobernanza de la protección (seguridad y ciberseguridad) será necesaria para garantizar que las autoridades portuarias, los armadores y todas las partes interesadas del sector marítimo dispongan de las herramientas, los conocimientos y la estructura necesarios para maximizar el rendimiento de la protección de sus infraestructuras (puertos, a bordo de sus buques) y alcanzar sus objetivos de protección, de conformidad con la legislación sobre protección marítima y las mejores prácticas internacionales.

4.4 Incidentes de seguridad y actores de amenazas

Cada puerto debe desarrollar una gobernanza de trabajo a su medida con prácticas eficaces de gestión de riesgos (físicos y cibernéticos) que garanticen la seguridad de las IC, las operaciones y los servicios marítimos.

4.4.1 Tipos de atacantes

Los ciberdelincuentes son adversarios que realizan una acción ilegal utilizando medios digitales. Por ejemplo, si el impacto del ataque es ilegal (por ejemplo, robo, crimen,

[14] Fuente: (Burt, 2021)

vandalismo, terrorismo) entonces se le caracteriza como ciberdelincuente. Los adversarios se clasifican a su vez en función de sus motivaciones, oportunidades y capacidades:

- *Actores intencionados*: los atacantes internos son una clase de amenazas con un conocimiento detallado de una organización y sus sistemas.
- *Ciberterroristas:* realizan actividades violentas para influir en la opinión pública y en la toma de decisiones.
- *Hacktivistas / Activistas civiles*: por razones ideológicas, realizan ataques para llamar la atención sobre una agenda política, social, religiosa o moral.
- *Ciberdelincuentes (organizados):* su objetivo es obtener un beneficio económico, influir en las elecciones, abusar de las personas. Todas las actividades delictivas tradicionales que se llevan a cabo utilizando medios digitales pertenecen a esta categoría.
- *Script Kiddies:* agentes no maduros con pocos conocimientos y capacidades, con el motivo habitual de divertirse, ganar una apuesta o un premio.
- Los *atacantes patrocinados por el Estado / espías* gubernamentales operan para obtener acceso a información privilegiada, como propiedad intelectual, planes de negocio, hojas de ruta, datos de personal o de clientes, etc. y conocer las operaciones empresariales y la próxima toma de decisiones.
- *Competidores / Agentes comerciales de espionaje industrial* intentan obtener una ventaja comercial mediante el robo de propiedad intelectual, documentación sobre operaciones y decisiones empresariales o datos de clientes.
- *Los ciberguerreros gubernamentales / cibercombatientes individuales* son tipos de actores con motivaciones patrióticas. Están controlados directamente por una nación o son individuos o grupos de personas movidos por sus valores políticos, sociales, étnicos o religiosos.
- La principal motivación de *los cibervándalos y los ciberpunks* es la destrucción de bienes, impulsados por la búsqueda de la satisfacción personal y el dominio.
- *Los Blackhat Hackers / Crackers* intentan acceder a los sistemas por curiosidad y beneficio personal, que puede ir desde recompensas económicas por explotar datos, productos y sistemas obtenidos, o en términos de reputación y reconocimiento entre sus pares.

También existen los *Actores involuntarios*, que suelen ser empleados sin formación o imprudentes que aún tienen potencial para causar daños a la organización. No tienen intenciones maliciosas, pero se mencionan porque sus acciones pueden representar un riesgo para la seguridad.

4.4.2 Incidentes de seguridad

Las operaciones portuarias y de los buques dependen cada vez más de la eficacia de los sistemas basados en software para las operaciones, y aquellos buques y puertos que puedan aprovechar las nuevas tecnologías y las soluciones digitales estarán en mejor situación que otros. Por ejemplo, la comunicación entre los buques y las operaciones portuarias de manipulación de la carga requiere la transferencia de información a través de ordenadores. Estos sistemas informáticos se encargan de todas las tareas administrativas de preparación, ejecución y manipulación de la carga. Las máquinas de manipulación de terminales, como las

grúas de contenedores, y la maquinaria a bordo de los buques tienen conexiones digitales con otros sistemas de control remoto. Estas máquinas mecánicas con equipos digitales se denominan sistemas de Tecnología Operativa (TO). En general, puede decirse que los sistemas de TO controlan el mundo físico, como las máquinas, mientras que los sistemas TI gestionan datos/información. Los segundos gestionan el flujo de información digital (datos), mientras que los primeros gestionan el funcionamiento de los procesos físicos y la maquinaria utilizada para llevarlos a cabo. En el mundo marítimo, TO se refiere al hardware, los sistemas y el software de los buques y puertos que hacen funcionar los buques y los equipos de manipulación portuaria y supervisan y controlan los dispositivos y procesos físicos, e TI se refiere a los ordenadores y servidores de las oficinas utilizados para gestionar el procesamiento de la información, incluidos el software, el hardware y las tecnologías de la comunicación.

Estos sistemas TO e TI no siempre están bien protegidos contra un ciberataque. Los riesgos de los sistemas informáticos afectan sobre todo a las finanzas y la reputación, mientras que los sistemas de TO pueden afectar y amenazar las infraestructuras portuarias e incluso costar vidas humanas. Los puertos marítimos y los buques pueden parecer objetivos inusuales de los ciberataques, pero estos ataques se dirigen cada vez más a los operadores marítimos y se informa regularmente de ataques con éxito en todo el mundo. Por ello, la ciberseguridad es cada vez más importante para resistir los ciberataques en el sector marítimo.

Durante mucho tiempo, la alta dirección de puertos y navieras ha considerado la ciberseguridad y la gestión de riesgos como una tarea del departamento informático, pero esto está cambiando rápidamente, ya que todo el personal participa en la gestión y ayuda a mitigar los riesgos cibernéticos.

El impacto de un ciberataque puede propagarse en los activos físicos. Por ejemplo, un ciberataque puede desactivar el sistema inteligente de detección de incendios y los sistemas automáticos de extinción de un buque metanero en un importante puerto de África y provocar un incendio. Los ciberataques y cualquier tipo de incidente de protección/seguridad pueden afectar negativamente a las cadenas de suministro marítimo y al comercio local e internacional. Por ejemplo, un ciberataque contra el sistema electrónico de navegación puede desorientar a un buque y hacer que colisione y se hunda a la entrada de un gran puerto de la UE o de África. Podría llevar semanas retirar los restos y devolver el puerto al servicio, con los perjuicios económicos, jurídicos y empresariales que la interrupción del comercio supone para las cadenas de suministro africanas y europeas.

Los barcos podrían utilizarse como medio de transporte de terroristas o para introducir armas de contrabando en un país, pero también podrían utilizarse para detonar una bomba en el barco y volar una zona crítica del puerto. Sin embargo, una encuesta sobre ciberseguridad de 2018[15] descubrió que pocas empresas navieras están preparadas para capear un ciberataque sin sufrir grandes daños. La necesidad de directrices y leyes pertinentes está más que clara en el sector. Los puertos deben aplicar un plan de gobernanza eficaz que abarque los procedimientos y procesos de gobernanza de la seguridad física y cibernética.

[15] (Jørgensen, 2018)

4.4.2.1 Accidentes de seguridad

Varios accidentes marítimos y catástrofes mortales de buques se consideran incidentes de seguridad. Por ejemplo, el hundimiento del RMS Titanic en abril de 1912 fue uno de los primeros buques de pasajeros que se hundieron con una pérdida de más de 1.500 vidas. Este desastre y el gran número de víctimas se debieron a una navegación imprudente cerca de icebergs y a la insuficiencia de botes salvavidas para salvar a todos los que iban a bordo.[16] Otro ejemplo es el hundimiento del transbordador M/S Estonia en 1994, en el que la visera de proa no estaba cerrada herméticamente y se abrió en una tormenta, lo que provocó el hundimiento y la pérdida de más de 850 pasajeros.[17] En 1987 se produjo un accidente similar con el transbordador Herald of Free Enterprise, que causó la pérdida de 197 personas y de todo el buque con su carga.[18] La fatal explosión del buque cisterna M/V Bow Mariner en 2004, cargado de etanol, explotó, se hundió y causó la muerte de 21 tripulantes. La razón de este desastre[19] fue la violación de varias normas de seguridad que provocaron la explosión y aumentaron el número de víctimas mortales. Un accidente más reciente, el desastre del Costa Concordia en 2012, se produjo cuando el capitán navegó demasiado cerca de las rocas, lo que provocó la pérdida del buque y de 32 vidas.[20]

En los puertos marítimos pueden producirse muchos accidentes relacionados con las operaciones de carga y descarga de los buques, pero también en las terminales y en la zona portuaria común. Un estudio realizado por R. Darbra y J. Casal[21] sobre cientos de accidentes ocurridos en puertos marítimos concluyó que los accidentes más frecuentes eran los escapes de gas (51%), seguidos de incendios (29%) y explosiones (17%). Más de la mitad de los accidentes se produjeron durante las operaciones de carga y descarga, pero los accidentes en almacenes, plantas químicas y operaciones dentro de la zona portuaria también contribuyeron significativamente al número total. Uno de los ejemplos más recientes de accidente grave se produjo en el puerto de Beirut en agosto de 2020, donde una enorme explosión que devastó partes de Beirut se atribuyó a la detonación de 2.750 toneladas de nitrato de amonio que se habían almacenado en el puerto de Beirut tras el apresamiento de un buque.[22]

4.4.2.2 Ciberataques

Los ciberataques contra las infraestructuras marítimas pueden ser variados. A continuación, se enumeran algunos ejemplos de ciberataques recientes con el fin de llamar la atención de los lectores sobre las amenazas potenciales de tales actos malintencionados y analizar más a fondo los mecanismos de estos ataques.

- El 10 de abril de 2020, un ataque de malware tuvo como objetivo la compañía naviera Mediterranean Shipping Company (MSC).[23] Por motivos de seguridad, los servidores

[16] (Titanic, n.d.)
[17] (Langewiesche, 2004)
[18] (Herald of Free Enterprise Ferry Disaster – 1987, n.d.)
[19] (Shapira, 2006)
[20] (Costa Concordia: What happened, 2015)
[21] (Darbra & Casal, 2004)
[22] (The Beirut Port Explosion, n.d.)
[23] (Hand, 2020)

de MSC se apagaron para proteger los datos de la empresa y el sitio web de MSC se desconectó. El ataque perturbó los procesos de datos internos.

- El 8 de julio de 2019, un ataque de malware tuvo como objetivo un barco con destino al puerto de Nueva York, lo que provocó la pérdida de datos críticos. La Guardia Costera informó de que la falta de estrategias de seguridad en el barco fue la principal razón de tal ataque.[24] Todos los tripulantes del barco compartían el mismo nombre de usuario y contraseña para el ordenador del barco. Además, el hacker se aprovechó del uso de dispositivos externos y de la falta de software antivirus.
- En marzo de 2019, un ataque de ransomware paralizó por completo la red global de la naviera Norsk Hydro al ser víctima del ransomware LockerGoga. Norsk Hydro calcula que los piratas llevaban en su red entre dos y tres semanas antes de ser descubiertos. Más de 22.000 ordenadores y miles de servidores de cinco países se vieron afectados, y LockerGoga paralizó la producción y las operaciones de oficina durante días. Los daños se estimaron en 71 millones de dólares.[25]
- En 2018, el gobierno chino es sospechoso de haber llevado a cabo un ataque de ransomware contra un contratista de la Marina estadounidense y haber robado datos de seguridad altamente sensibles, incluidos los planos de un proyecto de misiles supersónicos.[26]
- En septiembre de 2018, los ciberataques afectaron a los puertos de Barcelona (España) y San Diego (Estados Unidos). El ataque ransomware al puerto de San Diego resultó ser una infección del malware SamSam.[27] El impacto se limitó a algunas funciones administrativas de la autoridad portuaria y no interrumpió las operaciones portuarias ni los movimientos de los buques. El Puerto de Barcelona no reveló inmediatamente el tipo de incidente, pero indicó que el ataque había perturbado sus sistemas informáticos internos, aunque no afectó a las operaciones de los buques ni del puerto.
- En julio de 2018, China Ocean Shipping Company (COSCO) también fue víctima del ransomware SamSam. Cuando SamSam golpeó, interrumpió las redes de COSCO en Estados Unidos, Canadá, Panamá, Argentina, Brasil, Perú, Chile y Uruguay. La empresa tardó 5 días en volver a funcionar.
- A.P. Moller-Maersk Group sufrió un ataque devastador en junio de 2017 debido al malware NotPetya.[28] Maersk tuvo que interrumpir sus operaciones durante 10 días para recuperarse del ataque, lo que supuso reinstalar 4.000 servidores, 45.000 ordenadores y 2.500 aplicaciones. Al parecer, Maersk perdió unos 300 millones de dólares en ingresos.

La siguiente tabla enumera las principales amenazas cibernéticas para 2022 según la Agencia de la Unión Europea para la Ciberseguridad (ENISA) con la Gestión del Riesgo Cibernético de los Puertos.

[24] (Winder, 2019)
[25] (Tomter & Gundersen, 2019)
[26] (China hackers steal data from US Navy contractor - reports, 2018)
[27] (Port of San Diego: phishing emails remain amongst greatest cyber threats, 2021)
[28] (Greenberg, 2018)

Ciberamenazas	Incidente cibernético			Referencia
	Organización afectada	Fecha	Impacto	
Malware/ Ransomware	Gran terminal petrolera de Europa	2022	Sistemas informáticos	https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack
Malware/ Ransomware	Puerto de Amberes	2022	Compañías petroleras	https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892
Malware	Oil tanking Deutschland GmbH & Co. KG	2021	Sistemas informáticos	https://www.bbc.com/news/technology-60215252
Malware/ Ransomware (Mailto)	Grupo Toll	2020	Destrucción de datos	https://www.itnews.com.au/news/toll-group-hit-by-new-variant-of-mailto-ransomware-537537
Malware	Compañía Naviera Mediterránea (MSC)	2020	Interrupción de la red	https://www.wsj.com/articles/mediterranean-shipping-co-hit-by-network-outage-considering-potential-cyberattack-11586523861
Malware	CMA CGM	2020	Violación de la seguridad	https://www.reuters.com/article/uk-cma-cgm-cyber-idUKKBN26L2N0
Malware/ Ransomware	Servicios administrativos del puerto	2018	Puerto de San Diego y Barcelona	https://www.acronis.com/en-us/blog/posts/ransomware-attacks-sail-san-diego-and-barcelona/
Malware/ Ransomware	COSCO	2018	Avería de la red local	https://www.forbes.com/sites/leemathews/2018/07/26/another-shipping-giant-falls-victim-to-ransomware/?sh=6aa75bd70d04
Malware/ Ransomware (NotPetya)	A.P. Moller–Maersk	2018	Destrucción de datos	https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
Violación de datos	El servicio del puerto controlaba el movimiento y la ubicación de los contenedores	2013	Puerto de Amberes	https://www.bbc.com/news/world-europe-24539417

Los cambios geopolíticos también afectan a la seguridad de las operaciones marítimas. Durante la guerra de Ucrania de 2022, los buques que navegaban por el Mar Negro y el Mar de Azov sufrieron una serie de ciberataques. La Administración Marítima de Estados Unidos (MARAD) informó de que los buques se convirtieron en víctimas cibernéticas de interferencias del GPS, suplantación del SIA e interferencia de las comunicaciones. El Centro de Transporte Marítimo de la OTAN y la Administración Marítima de Estados Unidos informaron de ataques DDoS a estos buques.

4.4.2.3 Ataques de TI/TO

Muchos buques siguen utilizando sistemas y tecnologías de la información de TI y TO que no están concebidos para resistir ciberataques. Si no se protegen adecuadamente, los piratas informáticos pueden aprovecharse de las vulnerabilidades. Si pueden controlar el sistema del

buque a distancia, podrían apoderarse de los sistemas de información de comunicación de mando y control. Un buque es un sistema integrado de sistemas. Esta es la razón por la que es necesario definir y evaluar los sistemas de infraestructuras de información críticas del buque, así como supervisar su seguridad de forma continua e inspeccionarlos periódicamente. Otras actividades que podrían realizar los hackers son:

- burlar los sistemas de navegación
- controlar el piloto automático del buque
- interferir o saturar los radares de los barcos
- controlar los motores y la velocidad del buque
- desestabilizar los buques mediante la transferencia/inundación de agua de lastre
- dañar gravemente los equipos, por ejemplo, desconectando un sistema de refrigeración vital
- apagar sistemas de carga vitales como el suministro eléctrico de los frigoríficos
- apagar los sistemas de detección y extinción de incendios
- tomar el control del timón el tiempo suficiente para dirigir el barco hacia el muelle a toda velocidad

Por ello, los buques deben utilizar soluciones tecnológicas y principios operativos para evitar este tipo de situaciones. Las soluciones se describen en este estudio en los capítulos 5 y 6.

Lo mismo puede decirse de los puertos en los que también se utilizan constantemente sistemas de TI y TO. En el ámbito de la protección de los puertos y las terminales que cumplen las normas PBIP, es importante tener en cuenta lo siguiente:

- el Sistema de Gestión de la Seguridad (SGS) sólo es eficaz si está digitalizado.
- el sistema de tarjetas identificativas es eficaz cuando se trata de un sistema digital basado en una base de datos común a la que también tienen acceso las fuerzas del orden y las aduanas.
- el sistema automático de barrera sólo admite a las personas con derecho a entrar en la zona.
- un sistema de vigilancia perimetral con un circuito cerrado de televisión (CCTV) de alto rendimiento u otro sistema de cámaras tomará medidas inteligentes y podrá realizar un seguimiento de las secuencias de vídeo durante largos periodos de tiempo.

A continuación, se incluyen más detalles al respecto.

4.4.2.4 El uso de ordenadores para comunicarse entre las partes interesadas permite actuar en tiempo real y con eficacia cuando es necesario. Cadena de suministro y amenazas híbridas

Las cadenas de suministro marítimas son esenciales para el comercio y la economía mundiales, e implican la colaboración transfronteriza para ofrecer servicios complejos críticos (por ejemplo, gestión de contenedores, transporte de vehículos, almacenamiento y transporte de GNL, cruceros). La mayoría de los procesos físicos dentro de un servicio marítimo (por ejemplo, vehículos y carga/descarga de mercancías, distribución y almacenamiento de GNL) se ejecutan con sistemas físicos mecánicos autónomos o semiautónomos y maquinarias (por ejemplo, buques, camiones, grúas, puertas/barreras

electrónicas) bajo el control de sofisticados sistemas de software logístico (por ejemplo, sistemas ciberfísicos industriales, SCADA, sistemas de vigilancia). Además, los buques de carga están conectados con los puertos y los demás operadores a través de una plétora de enlaces de comunicación y datos (por ejemplo, comunicaciones por satélite o radiocomunicaciones convencionales) y su navegación depende hoy en día en gran medida de soluciones electrónicas (por ejemplo, navegación por satélite con GPS, Galileo o Sistemas de Información de Visualización de Cartas Electrónicas, (ECDIS)). Así pues, las cadenas de suministro marítimas pueden considerarse complejos sistemas físico-cibernéticos compuestos por activos físicos y cibernéticos heterogéneos e interconectados, propiedad de diferentes IC nacionales, de la UE e internacionales, que garantizan un intercambio de productos/datos rápido y sin fisuras desde el productor hasta el consumidor final durante la prestación de estos servicios.

La interconexión de los activos físicos y cibernéticos expone al ecosistema marítimo a **amenazas híbridas** en las que los ataques a los activos físicos se propagan a los cibernéticos y viceversa.

Los ataques a los servicios de la cadena de suministro marítima causan no sólo la interrupción de los servicios, sino un daño tremendo a las operaciones marítimas, la seguridad internacional, las economías, las sociedades y el medio ambiente. Por ejemplo, los ataques en los sistemas de control industrial (ICS) (p. ej. control de supervisión, SCADA, sistemas de control distribuido y controladores lógicos programables) alojados en puertos o empresas de transporte marítimo pueden causar interrupciones o daños en dispositivos mecánicos críticos (p. ej. grúas de contenedores, sistemas mecánicos y de seguridad que hacen funcionar esclusas y presas) y, lo que es peor, pueden provocar la pérdida de vidas humanas, el robo de la carga o la destrucción de un buque. Los efectos (en términos de radiación térmica, onda expansiva de sobrepresión y metralla voladora) de la explosión de un buque metanero o en las instalaciones o terminales de almacenamiento de GNL de los puertos debido a un sistema SCADA pirateado, podrían provocar una pérdida de reservas de energía, que podría ser crítica durante el invierno. También podría repercutir negativamente en el medio ambiente (degradación, fragmentación o pérdida de ecosistemas), la economía y, lo que es más importante, el bienestar y la salud de los ciudadanos. Un ataque al sistema de gestión de una terminal de contenedores podría interrumpir los servicios intermodales de contenedores que implican el transporte marítimo, ferroviario y por camión.

Los ciberataques (p. ej. la inserción de un malware) en los sistemas SCADA de los puertos pueden provocar vertidos de combustible que afecten a la calidad del agua; los ataques en el PCS pueden convertir los buques cisterna de GNL en bombas flotantes; los ataques físicos (p. ej. la colocación de una bomba) en una zona de almacenamiento de productos del carbón a granel seco pueden crear y transportar polvo por el viento a las terminales turísticas o a las residencias cercanas. Los modernos sistemas de vigilancia, unidades de control, sensores, Identificadores por radiofrecuencia (RFIDs), sistemas de tráfico marítimo, PCS, sistemas automatizados de control fronterizo son susceptibles de sufrir las amenazas actuales. Son propensos al fisgoneo, la interrupción, el vandalismo y la interceptación, lo que puede causar la interrupción de diversas operaciones y servicios marítimos críticos, así como su uso en el tráfico de personas y drogas y el terrorismo. Cabe señalar que, según estimaciones de 2016

de la RAND Corporation y del Servicio de Investigación del Congreso de Estados Unidos, un ataque a la IC de un puerto podría causar decenas de miles de muertes y paralizar el comercio mundial, con pérdidas que oscilarían entre 45.000 millones de dólares y más de un billón de dólares.

La Asociación Internacional de Sistemas de Comunidades Portuarias recomendó en 2015 que todos los agentes marítimos, logísticos, de la cadena de suministro y operadores de PCS -con el apoyo de sus asociaciones comerciales y organismos internacionales y regionales- aborden las amenazas actuales a la cadena de suministro. Además, recomendó reunir a las principales partes interesadas de la cadena de suministro para crear un Centro de Análisis e Intercambio de Información (ISAC) en el que debatir las amenazas, los riesgos y las experiencias en materia de ciberseguridad.

ENISA ha publicado las amenazas más importantes para la cadena de suministro, que se muestran a continuación.[29]

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos de los proveedores objeto del ataque a la cadena de suministro
Infección por malware	Software preexistente
Ingeniería social	Bibliotecas de software
Ataque de fuerza bruta	Código
Explotación de la vulnerabilidad del software	Configuración
Explotación de la vulnerabilidad de la configuración	Datos
Inteligencia de fuentes abiertas (OSINT)	Procesos
	Hardware
	Personas
	Proveedor

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente objeto del ataque a la cadena de suministro
Relación de confianza [T1199]	Datos
Compromiso por descarga desapercibida [T1189]	Datos personales
Phishing [T1566]	Propiedad intelectual
Infección por malware	Software
Ataque físico o modificación	Procesos
Falsificación	Ancho de banda
	Fianciero
	Personas

Figura 7: Taxonomía propuesta por ENISA para los ataques a la cadena de suministro.

Consta de cuatro partes: (i) técnicas de ataque utilizadas contra el proveedor, (ii) activos atacados del proveedor, (iii) técnicas de ataque utilizadas contra el cliente, (iv) activos atacados del cliente.

[29] (Threat Landscape for Supply Chain Attacks, 2021)

4.4.2.5 Vectores de amenaza

Basándose en múltiples recursos [30,31,32,33,34 y 35] a continuación se enumeran las amenazas habituales a la ciberseguridad marítima y los activos marítimos que son objetivo de técnicas específicas:

Amenazas	Técnicas	Activos y servicios marítimos como objetivos
Ransomware	Acceso inicial	Personas, sistemas informáticos, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, etc.
	Ejecución	Sistemas de TI, dispositivos finales de TI, componentes de redes y comunicaciones, etc.
	Persistencia	Personas, servicios de la autoridad, servicios de apoyo, etc.
	Escalada de privilegios	Personas, sistemas informáticos, dispositivos finales de TI, etc.
	Defensa evasión	Sistemas de TI, dispositivos finales de TI m componentes de redes y comunicaciones, infraestructura móvil, infraestructura fija, etc.
	Acceso con credenciales	Personas, sistemas informáticos, dispositivos finales de TI, etc.
	Descubrimiento	Personas, sistemas informáticos, dispositivos finales de TI, componentes de redes y comunicaciones, etc.
	Movimiento lateral	Personas, sistemas informáticos, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, etc.
	Colección	Información y datos, servicios de atraque de buques, servicios de protección y seguridad, personas, servicios de apoyo, servicios de almacenamiento temporal y estanciam servicios de distribución y transferencia, etc.
	Mando y control	Sistemas de TI, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, servicios de atraque de buques, servicios de carga y descarga de buques, servicios de distribución y transferencia, infraestructura móvil, infraestructura fija, sistemas y redes TO, etc.
	Exfiltración	Dispositivos finales de TI, sistemas informáticos, componentes de redes y comunicaciones, sistemas y redes TO, etc.
	Impacto	Sistemas informáticos, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, etc.
Malware	Violación de la seguridad	Dispositivos finales de TI, sistemas informáticos, información y datos, etc.
Ingeniería social	Reconocimiento	Personas, sistemas informáticos, servicios de autoridades, servicios de seguridad, sistemas de seguridad, etc.

[30] (Ashraf, et al., 2022)
[31] (ENISA Threat Landscape 2022, 2022)
[32] (Guidelines - Cyber Risk Management for Ports, 2020)
[33] (Alcaide & Garcia-Llave, 2020)
[34] (Meland, Bernsmed, Wille, Rødseth, & Nesheim, 2021)

	Desarrollo de recursos	Personas, sistemas informáticos, servicios a las autoridades, sistemas de seguridad, información y datos, etc.
	Acceso inicial	Personas, sistemas de TI, sistemas y redes de TO, dispositivos finales de TI, dispositivos finales de TO, etc.
	Ejecución	Personas, sistemas informáticos, etc.
Amenazas contra la disponibilidad (DDoS)	Desarrollo de recursos	Sistemas de TI, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, infraestructura móvil, infraestructura fija, etc.
	Defensa evasión	Sistemas informáticos, dispositivos finales de TI, componentes de redes y comunicaciones, etc.
	Impacto	Sistemas de TI, dispositivos finales de TI, componentes de redes y comunicaciones, información y datos, infraestructura móvil, infraestructura fija, servicios de atraque de buques, servicios de carga y descarga de buques, servicios de distribución y transferencia, servicios de apoyo, servicios de autoridades, servicios de seguridad, etc.
Amenazas contra la disponibilidad (Amenazas de Internet)	Acceso inicial	Dispositivos finales de TI, sistemas informáticos, componentes de redes y comunicaciones, etc.
	Descubrimiento	Dispositivos finales de TI, sistemas informáticos, componentes de redes y comunicaciones, etc.
	Colección	Dispositivos finales de TI, sistemas informáticos, componentes de redes y comunicaciones, etc.
	Impacto	Dispositivos finales de TI, sistemas informáticos, componentes de redes y comunicaciones, etc.
Desinformación - Información errónea	Reconocimiento	Personas, dispositivos finales de TI, sistemas informáticos, información y datos, etc.
	Desarrollo de recursos	Personas, dispositivos finales de TI, sistemas informáticos, información y datos, etc.
	Acceso inicial	Personas, dispositivos finales de TI, sistemas informáticos, etc.
	Ejecución	Personas, dispositivos finales de TI, sistemas informáticos, etc.
	Impacto	Personas, dispositivos finales de TI, sistemas informáticos, etc.
Ataques a la cadena de suministro	Reconocimiento	Tanto proveedores como clientes (cuadro del panorama de amenazas para los ataques a la cadena de suministro)
	Desarrollo de recursos	Tanto proveedores como clientes (cuadro del panorama de amenazas para los ataques a la cadena de suministro)
	Acceso inicial	Tanto proveedores como clientes (cuadro del panorama de amenazas para los ataques a la cadena de suministro)

5 Normas y estrategias de seguridad marítima

En este capítulo se presentan los organismos de normalización y las instancias políticas, y se esbozan las normas de protección marítima (seguridad y ciberseguridad) y su objetivo.

5.1 Introducción

Durante más de una década, se han realizado importantes esfuerzos en la introducción de metodologías de gestión y aseguramiento de riesgos para las ICI, concentrándose o bien en las amenazas cibernéticas o bien en las físicas, ignorando la compleja naturaleza dual (física y cibernética) de las ICI marítimas. En este capítulo se resumen las normas de protección marítima pertinentes y, en la última sección, se dan orientaciones sobre qué utilizar para cada amenaza.

5.1.1 Estrategia de Seguridad Marítima de la UE (ESMUE)

La primera Estrategia de Seguridad Marítima se adoptó el 24 de junio y el 16 de diciembre de 2014 como respuesta a los modernos riesgos y amenazas para la seguridad marítima mundial. La Estrategia promueve una mejor cooperación y coordinación entre civiles y militares y entre agentes de seguridad internos y externos, como la policía y la defensa. El objetivo es que este enfoque conjunto de la seguridad marítima fomente una cooperación más estrecha entre los distintos sectores marítimos y haga más coherente, eficaz y rentable la política de seguridad marítima de la UE. Esta herramienta explica cómo debe aplicarse el Plan de Acción y destaca las actividades del Servicio Europeo de Acción Exterior (SEAE) y el papel de las delegaciones de la UE y los servicios centrales del SEAE.

La Estrategia revisada de seguridad marítima de la UE adoptada en junio de 2018 permite un proceso de información más centrado para mejorar la concienciación y un mejor seguimiento de la Primera estrategia. El plan de acción reúne los aspectos internos y externos de la seguridad marítima de la Unión, facilita un enfoque estratégico e intersectorial y establece un programa conjunto civil-militar de investigación sobre seguridad marítima (incluido el doble uso).

La Estrategia revisada subraya que debe garantizarse una mejor coordinación en la aplicación de las estrategias y políticas de la UE con objetivos transversales, como las relativas a la energía, el medio ambiente y las amenazas y retos a la seguridad, incluidas las amenazas cibernéticas e híbridas, el terrorismo y la delincuencia organizada. Destaca la naturaleza cambiante de las amenazas en el ámbito marítimo y pide un compromiso renovado para la protección de las infraestructuras marítimas críticas, incluidas las submarinas, y las de transporte marítimo, energía y comunicaciones, entre otras cosas mejorando la concienciación marítima mediante la mejora de la interoperabilidad y la racionalización del intercambio de información (obligatorio y voluntario). Insta a mejorar la protección y la resiliencia de los sistemas e infraestructuras marítimos. A este respecto, se estudian las políticas e iniciativas pertinentes de la UE.

Una de las principales acciones mencionadas es la revisión de A.3.8: "Mejorar la integración de una dimensión de ciberseguridad en el ámbito marítimo en términos de capacidades, investigación y tecnología e industria, basándose en la coordinación civil-militar y las sinergias con las ciberpolíticas de la UE relacionadas tanto con la ciberseguridad como con la

ciberdefensa, en consonancia con la Directiva NIS y las recomendaciones y normativas internacionales como SOLAS XI-2 y el Código PBIP y sus futuras actualizaciones. Esto incluirá el intercambio de mejores prácticas y el desarrollo de proyectos conjuntos de los Estados miembros de la UE sobre prevención de ciberataques marítimos."

La acción A.4.3 establece: "Aplicar un enfoque global a la gestión de los riesgos para la protección marítima, en particular mediante la realización de análisis de riesgos comunes y la identificación de posibles lagunas y solapamientos en este ámbito, teniendo también en cuenta las amenazas cibernéticas e híbridas, los retos climáticos y las catástrofes medioambientales marítimas".

La acción A.4.8 establece: "Desarrollar una red de expertos en ciberseguridad y ciberdefensa para el ámbito marítimo con el fin de elaborar directrices sobre procedimientos en respuesta a las amenazas emergentes en el ámbito marítimo, incluidos posibles actos de terrorismo y otros actos ilícitos intencionados en el mar, especialmente en lo que respecta a la protección de los buques, la carga, la tripulación y los pasajeros, los puertos y las instalaciones portuarias, las instalaciones de energía marina y otras infraestructuras marítimas y energéticas críticas, en consonancia tanto con la Directiva NIS como con el Código PBIP." La creación de capacidades y la mejora de la educación y formación en materia de ciberseguridad en el ámbito marítimo en colaboración con todas las partes interesadas (por ejemplo, la ONU, la Organización Internacional del Trabajo (OIT) y la OMI y la OTAN) también figura entre las acciones de la estrategia revisada (Acción A.5.1, A.5.6).

La EUMSS cubre tanto los aspectos internos como externos de la seguridad marítima de la Unión; contribuye a un dominio marítimo global estable y seguro, de acuerdo con la Estrategia Europea de Seguridad. La Dirección General (DG) MARE es el órgano de la Comisión Europea responsable del desarrollo de la estrategia con la colaboración de varias DG (por ejemplo, DG CNECT, DG MOVE, DG ECHO, DG RTD) y agencias (por ejemplo, Agencia Europea de Seguridad Marítima (AESM), ENISA). La Estrategia 2020 de la Unión Europea en materia de Seguridad promueve la autonomía estratégica y la resistencia de las cadenas de suministro de la UE en lo que respecta a productos, servicios, infraestructuras y tecnologías críticos.

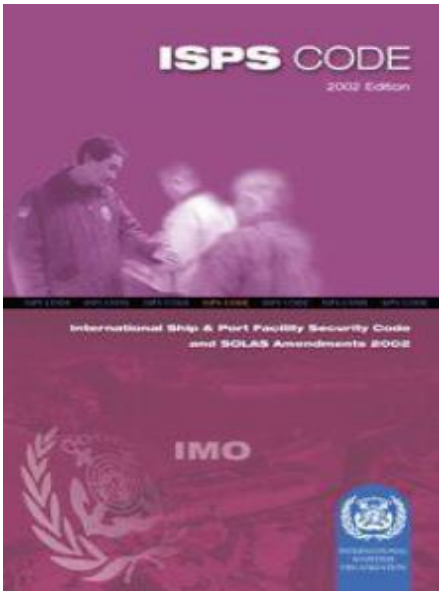
5.1.2 Normas de seguridad marítima

Las organizaciones marítimas (por ejemplo, OMI, BIMCO, AESM) han publicado diversas normas y directrices relacionadas con la seguridad, varias de las cuales se detallan a continuación.

5.1.2.1 Código PBIP

El más importante es el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP) de la OMI, que es el código internacional para la protección de buques e instalaciones portuarias, establecido por la OMI, dentro del reglamento del Convenio Internacional para la Seguridad de la Vida Humana en el Mar (SOLAS) de 1974 (capítulo XI-2).[35]

[35] (SOLAS XI-2 and the ISPS Code, n.d.)



El Código PBIP proporciona un marco a través del cual los buques y las instalaciones portuarias pueden cooperar para detectar e impedir actos que supongan una amenaza para la protección marítima. El Código ofrece un enfoque para establecer la gobernanza de la seguridad en las IC marítimas:

- permite detectar y disuadir las amenazas a la seguridad en un marco internacional;
- establece funciones y responsabilidades;
- permite recopilar e intercambiar información sobre seguridad;
- proporciona una metodología para evaluar la seguridad;
- garantiza la aplicación de medidas de seguridad adecuadas.

El código consta de dos partes con prescripciones obligatorias y directrices para la protección de los buques y las instalaciones portuarias. La parte A contiene requisitos obligatorios y la parte B recomendaciones de aplicación para mejorar la seguridad. En este sentido, los principios del Código PBIP son como el Código SIG a bordo de un buque. Antes de que el Código PBIP pueda aplicarse legalmente en un país, debe transponerse a la legislación nacional. Algunos países adoptaron el Código PBIP poco después de julio de 2004, pero otros no lo hicieron hasta años más tarde. Algunos países han adoptado el código en su totalidad, y otros han introducido variaciones en el Código PBIP nacional en relación con determinados aspectos de la protección portuaria.

La Unión Europea[36] aplicó inmediatamente la parte A del código en sus puertos y decidió tratar también la parte B como obligatoria y no como una mera recomendación. Los países africanos aplicaron el código de forma independiente a través de su legislación nacional.

Es importante destacar que el Código PBIP utiliza la palabra "instalación portuaria", lo que significa que el puerto no está bajo el paraguas PBIP. Los aspectos de protección "portuaria" se abordan en el Código de [Buenas] Prácticas (CBP) sobre Protección Portuaria.

[36] Directiva 2005/65/CE de mejora de la protección portuaria y las zonas adyacentes

El CBP de Ginebra de 2003 sobre protección portuaria complementa las disposiciones del Código PBIP en lo que se refiere a garantizar la protección de la zona portuaria en sentido amplio. El código define las funciones, obligaciones y medidas de seguridad para disuadir y responder a los actos delictivos contra los puertos. Utiliza las mismas prácticas y principios que el Código PBIP y es una guía para toda la protección portuaria más allá de la zona de las instalaciones portuarias. La Unión Europea introdujo el código como directriz obligatoria[37] para mejorar su protección portuaria.

5.1.2.1.1 Seguridad en la construcción

Desde el momento en que se construye un buque, la seguridad comienza con el requisito de que el buque esté en condiciones de navegar antes de salir de tierra, tal y como exige Lloyds of London (P&I Club).[38] Cada buque mercante está registrado por un Estado de abanderamiento, ya sea el país de residencia del armador o un país con pabellón de conveniencia. Deben cumplir las normas, reglamentos y disposiciones marítimas del Estado de abanderamiento específico, de conformidad con las normas y disposiciones marítimas internacionales de la OMI, y deben estar certificados por una sociedad de clasificación.

Sin embargo, algunos pabellones de conveniencia han reducido la seguridad, no disponen de recursos suficientes para realizar inspecciones adecuadas y no imponen sanciones a los buques infractores. Esto da lugar a buques que no cumplen varios requisitos críticos de seguridad, pero a los que a veces se sigue permitiendo atracar en determinados puertos. Dado que estos buques inseguros se centran únicamente en reparar partes del buque cuando se producen defectos, en lugar de centrarse en el mantenimiento preventivo, el riesgo de accidente es alto.

5.1.2.1.2 Control del Estado rector de puerto (CERP)

Es responsabilidad del Estado de abanderamiento (el país donde está registrado el buque) garantizar que un buque cumple todas las normas de seguridad exigidas. El CERP actúa como respaldo eficaz de las inspecciones que realizan periódicamente los Estados de abanderamiento para detectar buques deficientes.

El CERP es, por tanto, la iniciativa de la OMI en materia de seguridad marítima (protección física) cuyo objetivo es verificar el cumplimiento de los convenios y normas internacionales por parte de los buques. Contribuyen a reducir el riesgo de peligrosidad de los buques. La función del CERP es poner de relieve los posibles riesgos para la protección (de seguridad y cibernéticos) y comunicarlos al Estado de abanderamiento del buque. Durante las inspecciones de buques, el CERP verifica que el estado del buque y su equipo de manipulación cumplen los requisitos de la normativa internacional de la OMI y que el buque está tripulado y es operado de conformidad con estas normas. Trabajan según una resolución de cooperación para los controles de buques y descargas (Resolución 682 17 de la OMI).[39]

[37] Directiva 2005/65/CE de mejora de la protección portuaria y las zonas adyacentes
[38] (Rulebook 2021)
[39] (Resolution A.682 (17), 1991)

5.1.2.1.3 Normas de seguridad de las operaciones de los buques

Los marinos son el factor humano que puede mantener bajos los riesgos a bordo. Esta función está dirigida por el responsable de seguridad a bordo, que se encarga de mantener actualizado el plan de gestión de la seguridad, utilizar un Sistema de Gestión de la Seguridad (SMS) y mantener alerta a la tripulación mediante formación en seguridad. La columna vertebral de la gobernanza de la seguridad es el SMS, ya que su principal objetivo es proporcionar un enfoque sistemático para gestionar los riesgos de seguridad en las operaciones de los buques. El SMS forma parte del código internacional de gestión de la seguridad (ISM)[40] y la OMI exige a los buques comerciales que establezcan procedimientos seguros de gestión de buques.

Uno de los aspectos más importantes para mantener la integridad del buque durante un viaje por mar es que la carga esté bien sujeta. Las fuerzas laterales y longitudinales sobre el buque creadas por el oleaje durante los temporales suponen un enorme riesgo para la estabilidad del buque debido a los riesgos de desplazamiento de la carga. Toda la carga debe estibarse y asegurarse de forma que el buque y la tripulación no corran peligro. Deben seguirse procedimientos adecuados de amarre y sujeción, de conformidad con el código de estiba y sujeción de la carga (CSS) de la OMI[41]. Si un ataque malintencionado hace que la carga no esté asegurada y se mueva libremente en la bodega, el riesgo de perder el barco y la tripulación es real.

5.1.2.1.4 Aspectos de seguridad curativa a bordo de los buques

En caso de que se produzca un accidente a bordo, es vital que la tripulación esté capacitada para minimizar inmediatamente el impacto del daño causado. Por ello, los miembros de la tripulación reciben formación sobre principios de gestión de crisis y procedimientos de respuesta de emergencia ante todo tipo de accidentes y sobre cómo combatir un incendio. El Código de Formación, Titulación y Guardia para la Gente de Mar (STCW)[42] y el Convenio SOLAS abordan estos aspectos en detalle, pero este ámbito de especialización queda fuera del alcance del presente estudio.

5.1.2.2 Otros códigos importantes

- Código Marítimo Internacional de Cargas Sólidas a Granel (Código IMSBC) de la OMI;
- Código internacional para la construcción y el equipo de buques que transporten productos químicos peligrosos a granel (Código CIQ);
- Código Internacional para el Transporte de Grano a Granel (Código Internacional de Granos);
- Código de Prácticas para la Seguridad de las Operaciones de Carga y Descarga de Graneleros (Código BLU);
- Código Marítimo Internacional de Mercancías Peligrosas (IMDG);

[40] (The International Safety Management (ISM) Code)
[41] (Code of Safe Practice for Cargo Stowage and Securing (CSS Code), n.d.)
[42] (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197, n.d.)

- AESM[43] proporciona herramientas a los agentes marítimos de la UE, por ejemplo, SIA, SafeSeaNet para el seguimiento del tráfico de buques, imágenes por satélite de CleanSeaNet para identificar la contaminación en el mar, EMCIP para centralizar datos sobre accidentes marítimos, herramientas de formación, etc.
- La Organización Europea de Puertos Marítimos[44] fomenta los puertos verdes y la eficiencia energética, y está especializada en directrices de seguridad y formación relacionadas con las operaciones de los buques en los puertos, por ejemplo: puerto de aprovisionamiento de GNL, recepción de residuos, carga y descarga de mercancías generales, contenedores y graneles, y movimientos de contenedores.
- La OIT[45] ha publicado el Repertorio de recomendaciones prácticas de la OIT sobre seguridad y salud en los puertos; el Repertorio de la OIT ofrece orientaciones pertinentes para la gestión, el funcionamiento, el mantenimiento y el desarrollo de los puertos.
- La Iniciativa para la Seguridad de los Contenedores (CSI) de la USC
- La Asociación Comercial Aduanera contra el Terrorismo (C-TPAT)
- El plan de seguridad de la tripulación
- El sistema automatizado de manifiestos (AMS)
- SafeSeaNet
- SIA

5.1.3 Normas de ciberseguridad

5.1.3.1 Normas ISO[46] para la seguridad de las ICI marítimas

ISO27000 proporciona definiciones de conceptos de seguridad. La norma ISO/IEC 27001 aborda los requisitos de seguridad física en términos de prevención del acceso no autorizado a la información de una organización y sus instalaciones pertinentes, que se dividen en dos grandes categorías: zonas seguras y seguridad de los equipos.

ISO/IEC 27001 también se ocupa del Sistema de Gestión de la Seguridad de la Información (SGSI) de una organización, que en el caso de este informe son las ICI del puerto. El cumplimiento de la norma ISO 27001 significa prácticamente que la organización, en nuestro caso el puerto, cumple los requisitos de la norma en el ámbito de la seguridad, que es vital para el buen funcionamiento del puerto en un entorno de seguridad frente a las amenazas del ciberespacio. Las ICI están bien protegidas. Además, aclara los términos de seguridad física, como el perímetro de seguridad física, los controles físicos de entrada y las instalaciones. Los requisitos de seguridad física también se identifican en la publicación especial 800-171 del NIST. La familia de normas ISO2800x proporciona directrices para la seguridad de la cadena de suministro y, en particular, para las cadenas de suministro

[43] (European Maritime Safety Agency , n.d.)
[44] (ESPO: The First Port of Call for European Transport Policy Makers in Brussels, n.d.)
[45] (ILO: International Labour Oeganization, n.d.)
[46] (Standards, n.d.)

marítimas. En el siguiente cuadro[47] se resumen las distintas normas ISO pertinentes para la protección marítima.

R/N	ISO	COMENTARIOS
1.	ISO 18788:2015	Sistema de gestión de operaciones de seguridad privada.
2.	ISO 9001 / BS 10800	Código de buenas prácticas para la prestación de servicios de seguridad.
3.	ISO/IEC 27001	Norma internacional para gestionar la seguridad de la información.
4.	ISO 27002:2013 (anterior ISO 17799:2000)	Norma general de seguridad de la información. Consta de catorce secciones (5 a 18), cada una de las cuales está estructurada de la misma manera.
5.	ISO/IEC TS 30104:2015	Tecnología de la información - Técnicas de seguridad - Ataques a la seguridad física, técnicas de mitigación y requisitos de seguridad.
6.	ISO 28000:2007	Especifica los requisitos de un sistema de gestión de la seguridad, incluidos los aspectos críticos para garantizar la seguridad de la cadena de suministro.
7.	ISO 28000:2022	Seguridad y resiliencia - Sistemas de gestión de la seguridad – Requisitos.

Dado que los buques autónomos y las aplicaciones marítimas innovadoras utilizan la IA, es necesario tener en cuenta varias normas adicionales para el desarrollo de un ecosistema marítimo basado en la IA que sea digno de confianza.

A continuación, se mencionan las principales normas sobre IA:

5.1.3.2 Normas ISA, ANSI para ACS

Las normas ISA y ANSI tienen por objeto la seguridad de los sistemas de automatización y control industrial (ACS, por ejemplo, SCADA). Ejemplos de estas normas son:

- ISA-TR62443-2-3-2015 Seguridad para sistemas de automatización y control industrial, Parte 2-3: Gestión de parches en el entorno SIGC
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 Seguridad para los sistemas de automatización y control industrial, Parte 2-4: Requisitos del programa de seguridad para proveedores de servicios SIGC (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020 Seguridad para sistemas de automatización y control industrial, Parte 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas
- ANSI/ISA-62443-4-1-2018 Seguridad para sistemas de automatización y control industrial, Parte 4-1: Requisitos del ciclo de vida del desarrollo de productos seguros

5.1.3.3 Categorización de las normas

Existen numerosas normas de seguridad de diversos organismos de normalización (por ejemplo, ISO, OMI, ETSI, NIST, BIMCO, IEEE) que abordan diversos temas. Estos esfuerzos fragmentados crean confusión sobre qué norma(s) utilizar. Es necesario aclarar las complementariedades y los solapamientos. Para contribuir a esta aclaración, se ha facilitado

[47] Y. Papagiannopoulos, "Standards in Practice", IEEE Conference on Standards for Communications and Networking, noviembre de 2022.

una clasificación de las normas[48] en la que se han identificado las siguientes diez categorías de normas:

1. Vocabulario y conceptualización: normas que pueden utilizarse para fijar terminologías y describir conceptos.
2. Requisitos de seguridad: normas que establecen los requisitos de seguridad.
3. Directrices de seguridad: normas que proporcionan buenas prácticas.
4. Evaluación y valoración de la seguridad: normas y buenas prácticas relacionadas con las metodologías de evaluación o valoración de la seguridad.
5. Privacidad y protección de datos: normas relacionadas con el mantenimiento de la privacidad y la protección de datos.
6. Normas de gestión de riesgos: normas y buenas prácticas que proporcionan principios, marcos o procesos relacionados con la gestión de riesgos para la seguridad.
7. Normas técnicas: normas que abordan aspectos técnicos de seguridad.
8. IA y seguridad: Incluye normas, marcos y buenas prácticas relacionadas con la seguridad de la IA (importante para los buques autónomos, ahogos marítimos).
9. Específicas del sector (por ejemplo, transporte marítimo): normas de gestión de la protección que respaldan los requisitos específicos y las especificidades propias del sector (por ejemplo, sistemas de comunidad portuarios).
10. Protección de infraestructuras críticas: normas relacionadas con la protección de infraestructuras críticas para la sostenibilidad de la economía y el bienestar social (por ejemplo, las ICI marítimas).

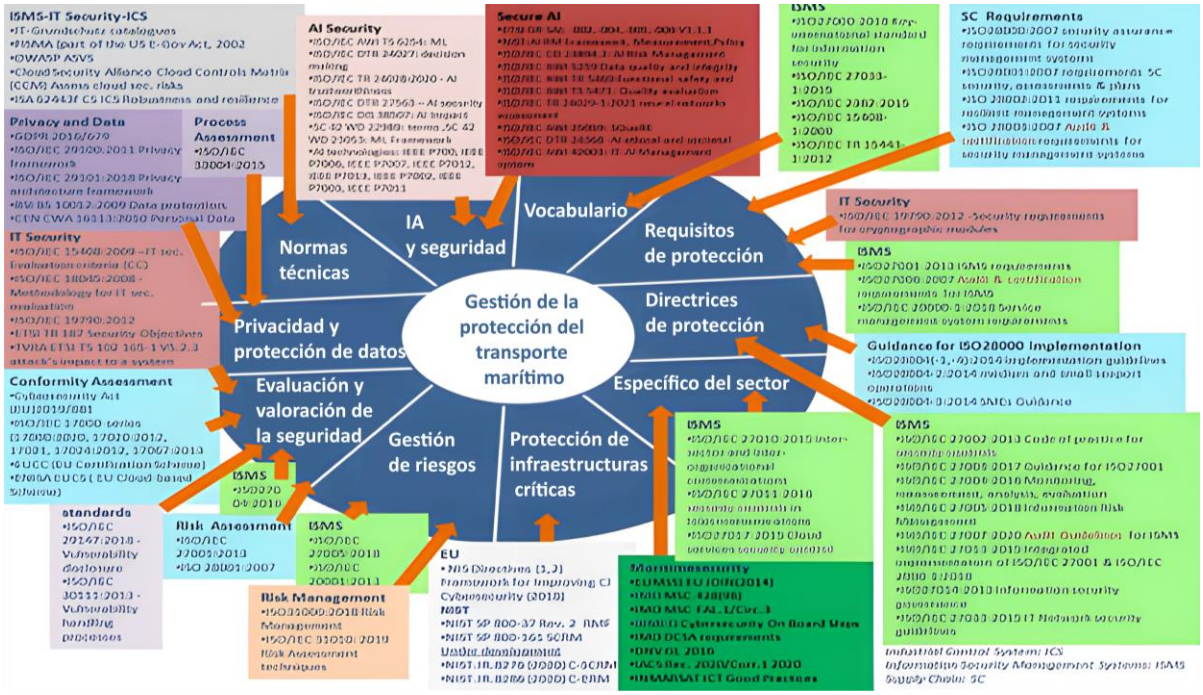


Figura 8: Taxonomía de las normas de seguridad marítima[49]

[48] (Kalogeri & Polemi, 2022)
[49] *Ibid.*

5.2 Legislación sobre seguridad

Las normas de seguridad en los puertos de todo el mundo (incluidos los africanos) no están, en principio, totalmente reguladas por las normas internacionales y siguen siendo decisión del Estado soberano. Cada país ha establecido su propia normativa de seguridad, lo que ha dado lugar a una variada cartera de leyes a veces diferentes y desfasadas.

Los principios de seguridad de la gobernanza portuaria son fundamentales, ya que implica a muchos responsables y partes interesadas, como la autoridad portuaria, los operadores de terminales, los operadores ferroviarios, las empresas de transporte por carretera, los proveedores de logística y los servicios de urgencias. A la hora de desarrollar un sistema de gestión de la seguridad portuaria, no sólo deben tenerse en cuenta los aspectos generales de seguridad dentro de la zona portuaria, sino también los aspectos de seguridad de la manipulación de la carga. No sería posible hacer justicia al tema aquí, pero un factor común es que la seguridad debe abarcar infraestructuras y equipos de manipulación de calidad, personal bien formado, un conjunto de procedimientos bien pensados y un SMS que supervise y haga un seguimiento de la situación real de seguridad. Es responsabilidad del responsable del puerto y de las instalaciones gobernar su SMS de forma profesional para evitar daños o perjuicios a las personas. El escudo de seguridad no debe volverse frágil, permitiendo daños consecuentes de ciberataques o ataques de seguridad.

La mayor parte de la legislación del mundo marítimo se ha iniciado a raíz de alguna catástrofe marítima, y en este caso, el desastre del Titanic dio lugar a la normativa internacional de seguridad SOLAS de 1974 como "escudo de seguridad" protector de marinos y buques. La amplia cobertura mediática, la posterior conmoción mundial causada por el enorme número de víctimas mortales y la demanda de los supervivientes contra la White Star Line condujeron a mejoras significativas de la seguridad en el mar.

Además de esta presión social, las compañías de seguros marítimos obligaron a las navieras a mostrar más liderazgo en la prevención de accidentes y convencieron a los gobiernos para que establecieran leyes de seguridad más eficaces. Se pasó de correr detrás de los hechos y pagar por los daños a una mentalidad de concienciación y prevención en materia de seguridad, que es vital para salvaguardar a las personas, más barata para las compañías de seguros y más eficaz para los armadores. El mundo marítimo sigue siendo una industria de alto riesgo con enormes consecuencias cuando algo sale mal.

La mejora más importante fue la creación del Convenio SOLAS, al establecer principios y normas uniformes para la construcción, instalación y explotación de buques mercantes. La versión actual del Convenio SOLAS de 1974[50] sigue siendo hoy la norma mundial para los buques y la gente de mar. Cada país, cada puerto y cada situación local son diferentes y exigen un planteamiento de riesgos complejo y personalizado para todas las operaciones, a fin de mitigar y minimizar los riesgos para la seguridad. Algunos países, como Australia, promueven el enfoque de liderazgo personalizado en materia de seguridad dentro de los puertos y se limitan a ofrecer orientaciones sobre buenas prácticas y a esbozar un modelo con el que medir las políticas, los procedimientos y el rendimiento de las operaciones portuarias.

[50] (International Convention for the Safety of Life at Sea (SOLAS), 1974, n.d.)

Dado que cada puerto tiene sus propios riesgos de seguridad, las normas de gestión de la seguridad sólo pueden abordarse desde el propio puerto y utilizar la normativa, las directrices y las mejores prácticas internacionales como herramienta para mejorar la seguridad en el puerto. En el mundo actual no es posible una única normativa internacional uniforme en materia de seguridad, sobre todo porque algunos países carecen incluso de lo básico al respecto.

Pero a diferencia de esta normativa de seguridad, la creación de una "legislación de seguridad" fue provocada por una catástrofe en tierra, cuando aviones secuestrados se estrellaron contra las torres gemelas del World Trade Center el 11 de septiembre de 2001.

En la actualidad, el sector marítimo se rige por varias normativas que obligan a los operadores marítimos a garantizar la seguridad y protección de los buques. Estas normas también se aplican a la ciberseguridad, y con la Resolución MSC.428(98) de la OMI, los riesgos de ciberseguridad deben abordarse ahora en el Sistema de Gestión de la Seguridad (SMS). Según las Directrices de la OMI para la gestión del riesgo cibernético marítimo (MSC-FAL.1 Circ.3)[51], "...el riesgo cibernético marítimo se refiere a una medida del grado en que una instalación tecnológica se ve amenazada por una circunstancia o evento potencial, que podría dar lugar a fallos operativos, de seguridad o de protección relacionados con el transporte marítimo debido a daños, pérdida o compromiso de los sistemas de información.".

Además de las directrices de la OMI, la Asociación Internacional de Puertos (IAPH) también ha elaborado una serie de directrices de ciberseguridad para puertos e instalaciones portuarias.[52]

Algunas de las normas europeas específicas de seguridad portuaria implicadas son:

- Directiva 2000/59/CE del Parlamento Europeo y del Consejo, de 27 de noviembre de 2000, sobre instalaciones portuarias receptoras de desechos generados por buques y residuos de carga.
- Directiva 2001/96/CE del Parlamento Europeo y del Consejo, de 4 de diciembre de 2001, por la que se establecen requisitos y procedimientos armonizados para la seguridad de las operaciones de carga y descarga de graneleros.
- Directiva 2000/59/CE del Parlamento Europeo y del Consejo, de 27 de noviembre de 2000, sobre instalaciones portuarias receptoras de desechos generados por buques y residuos de carga.

5.3 Legislación sobre ciberseguridad

La UE ha adoptado y mejorado el Código PBIP con dos directivas: la CE / 725 /2004 para las instalaciones portuarias y la CE / 65 / 2005 para los puertos. La UE protege sus infraestructuras (incluidas las ICI marítimas) mediante diversos instrumentos jurídicos:

[51] (Guidelines on Maritime Cyber Risk Management, 2017)
[52] (Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2021)

La *Directiva NIS* estableció una competencia europea en materia de ciberseguridad para proteger el mercado único digital; tiene tres objetivos principales: a) Mejorar las capacidades nacionales de ciberseguridad, exigiendo a todos los Estados miembros que dispongan de un conjunto mínimo común de capacidades de base. Esto incluye equipos de respuesta a incidentes de seguridad informática (CSIRT) dotados de recursos adecuados. b) Facilitar la cooperación transfronteriza a escala de la UE entre los Estados miembros y la Unión tanto a nivel estratégico/político como operativo en materia de ciberseguridad. Esto implica tanto al Grupo de Cooperación NIS como a la Red CSIRTs. Y c) promover una cultura de gestión de riesgos y notificación de incidentes entre los principales agentes económicos, en particular los operadores de servicios esenciales (OSE) para el mantenimiento de las actividades económicas y sociales y los proveedores de servicios digitales (PSD).

La *Ley de Ciberseguridad de la UE* establece un marco de certificación de ciberseguridad para productos y servicios. Este marco proporcionará sistemas de certificación a escala de la UE como un conjunto completo de reglas, requisitos técnicos, normas y procedimientos. De este modo será posible garantizar la confianza del público en la ciberseguridad de los productos y servicios informáticos. Es importante que pueda demostrarse que un producto ha sido comprobado y certificado para ajustarse a normas estrictas de ciberseguridad. Los productos relacionados con la IA ganarán en fiabilidad si están certificados y, en los próximos años, se desarrollarán diversos esquemas de ciberseguridad para los productos de IA que especifiquen los requisitos de seguridad.

El *Reglamento General de Protección de Datos (RGPD*) establece normas de protección de datos que explican qué, cómo y cuándo las personas pueden acceder a información sobre ellas y establece limitaciones sobre lo que las organizaciones pueden hacer con los datos personales.

El *Nuevo Marco Legislativo (NML)* mejora la vigilancia del mercado, introduce normas para proteger mejor tanto a los consumidores como a los profesionales de los productos inseguros (comunitarios o extracomunitarios), fija normas para la acreditación y establece un marco jurídico común para los productos industriales. El NML mejorará la seguridad de los productos basados en IA.

La *Ley de Chips* es relevante para la seguridad de la IA porque los semiconductores son la tecnología de plataforma del siglo XXI que se utilizará para el desarrollo de la IA y para incorporar fuertes medidas de seguridad. La industria globalizada de semiconductores de la UE se verá respaldada con esta propuesta de Ley.

La *Ley de Ciberresiliencia* establecerá a su debido tiempo nuevas normas de ciberseguridad para los productos digitales y los servicios auxiliares. Esta iniciativa fomentará también la seguridad de los productos de IA, ya que pretende responder a las necesidades del mercado y proteger a los consumidores de productos inseguros mediante la introducción de normas comunes de ciberseguridad para fabricantes y vendedores de productos digitales tangibles e intangibles.

6 Buenas prácticas de seguridad marítima

6.1 Introducción

Las IC marítimas (puertos o buques) deben considerarse infraestructuras físico-cibernéticas. Existen varias directrices para la seguridad de las IC marítimas:

- **ENISA Buenas prácticas de ciberseguridad en el sector marítimo** (2019)
- **ETSI TR 103 456** CYBER; Aplicación de la NIS **COM(2017) 476 final** "Sacar el máximo partido de la NIS"
- **C(2017)6100 final** Recomendación sobre la respuesta coordinada a incidentes y crisis de ciberseguridad a gran escala (proyecto)
- **Autoevaluación de la gestión de buques cisterna - TMSA** (OCIMF)
- **Las Directrices sobre ciberseguridad a bordo de los buques** (apoyadas por: **BIMCO**, CLIA, **ICS**, INTERCARGO, INTERTANKO, OCIMF e IUMI)
- **Concienciación sobre ciberseguridad** - AMMITEC

Este capítulo subraya los pasos que deben seguirse a nivel personal, organizativo y operativo para abordar de forma holística los retos de la seguridad. La seguridad se considera una responsabilidad conjunta y todas las partes implicadas deben adoptar buenas prácticas de ciberseguridad. Se han elaborado dos cuestionarios (véanse Anexos A y B) que se distribuirán en el futuro a los operadores marítimos para captar su nivel de concienciación en materia de seguridad.

6.2 Gobernanza de la seguridad marítima

La higiene de la seguridad de una IC marítima (por ejemplo, puerto, buque, compañía marítima) forma parte integrante de la estructura global de la IC. La higiene de la seguridad son todas estas medidas que deben adoptarse para que la IC marítima pueda funcionar con un nivel de riesgo aceptable frente a las amenazas físicas, cibernéticas, híbridas y a la cadena de suministro. Para comprender mejor la higiene de la seguridad de una IC marítima, primero hay que saber quiénes son las principales autoridades y partes interesadas que intervienen en la estructura general, las operaciones, los servicios y los usuarios internos y externos. También es necesario identificar todos los activos físicos y cibernéticos de la IC marítima, sus interconexiones, su interacción y su importancia (valor) para las operaciones de la IC. Es necesario asignar un propietario a cada activo que será responsable de su seguridad (un propietario puede ser responsable de varios activos).

Una IC marítima es un sistema de sistemas integrado en una entidad. Para entender mejor el ecosistema de la IC es necesario comprender quién participa en la gestión de activos. Esto es importante, ya que indica la gobernanza de la seguridad de la información de una IC marítima y las medidas generales de seguridad que deben adoptarse para proteger estos activos.

Toda IC marítima debe aplicar y practicar un esquema de gobernanza de la seguridad de la información, tal como se indica a continuación:

- Políticas (obligatorias)
- Normas (obligatorias)
- Directrices (no obligatorias)
- Procedimientos (obligatorios)
- Líneas de base (obligatorias)

Las políticas, normas, directrices y procedimientos establecen la gobernanza de la seguridad de una organización. A este respecto, la higiene de la seguridad de una organización puede lograrse mediante la aplicación de los elementos de la gobernanza de la seguridad y el establecimiento de un Sistema de Gestión de la Seguridad de la Información bien protegido, basado en (i) los controles de seguridad adecuados, (ii) la aplicación de los controles de seguridad (iii), la evaluación de los controles de seguridad en el entorno marítimo que se están aplicando, y (iv) el seguimiento periódico de su eficacia. La higiene de la seguridad debe aplicarse basándose en el enfoque de gobernanza de la seguridad descrito anteriormente.

La estructura de gobernanza debe aplicarse a ambos aspectos de la protección (seguridad y ciberseguridad) con un enfoque uniforme y debe ser parte integrante de todas las actividades de IC marítima. Los procedimientos de gobernanza deben incluir un Análisis de Impacto en el Negocio (BIA), una Evaluación de Riesgos actualizada y una Política de Seguridad. A este respecto, la gobernanza de la seguridad de la información debe supervisarse y evaluarse periódicamente sobre la base de Indicadores Clave de Rendimiento (KPI) e Indicadores Clave de Riesgo (KRI) de la seguridad física y cibernética y de la seguridad del personal. Un equipo de gestión de incidentes debe formar parte del equipo de gobernanza de la seguridad que será responsable de la previsión, identificación, análisis, mitigación y recuperación de cualquier incidente de seguridad (físico, cibernético, híbrido).

Es necesario establecer una autoridad central, con el mandato de supervisar la aplicación de la gobernanza de la seguridad de la información mediante la inspección (control de seguridad de la conducta) del sistema general de seguridad de la IC marítima.

6.3 Higiene de ciberseguridad de los operadores

Los datos del Informe de Investigaciones de Brechas de Datos 2019 (DBIR) de Verizon indican que casi un tercio (32%) de todas las brechas de datos involucraron estafas de phishing.[53] Cada 20 segundos se lanza un nuevo sitio de phishing, según se menciona en el informe 2020 Mobile Threat Landscape Report, de Wandera. El error humano causó el 90% de las violaciones de datos cibernéticos en 2019, según el análisis de datos de la Oficina del Comisionado de Información del Reino Unido (ICO) realizado por CybSafe. Según este análisis, nueve de cada diez de las 2.376 ciberinfracciones notificadas al ICO el año pasado fueron causadas por errores cometidos por los usuarios finales. Los ataques de phishing representan más del 80% de los incidentes de seguridad notificados; cada minuto se pierden 17.700 dólares debido a ataques de phishing; el 60% de las infracciones tenían que ver con

[53] (Widup, 2019)

vulnerabilidades para las que existía un parche pero que los administradores no habían aplicado.

Es necesario que todos los operadores marítimos y usuarios individuales apliquen buenas prácticas de seguridad personal estableciendo las normas y los esfuerzos necesarios para:

- Crear una cultura de seguridad e higiene cibernética
- Fomentar el intercambio de información y la colaboración
- Implicar a los operadores y usuarios en las decisiones y procedimientos relacionados con la seguridad
- Utilizar carteles y recordatorios
- Una formación práctica continua en seguridad a todos los niveles (desde seminarios hasta ejercicios)
- Un control de acceso eficaz
- Aplicar políticas de autenticación y contraseñas

6.4 Gestión de la seguridad marítima

La gestión de los riesgos físicos, cibernéticos e híbridos requiere un enfoque holístico. Los pasos generales que deben darse durante la gestión de la protección (seguridad y ciberseguridad) de una IC marítima son los siguientes:

1) Identificar los activos (físicos y cibernéticos) y asignar la propiedad, por ejemplo, asignar una persona o personas que serán responsables del activo.
2) Crear un inventario de activos actualizado dinámicamente (enumerar la propiedad).
3) Categorizar y clasificar los activos en función de:
   - Valor del bien (importancia para la IC marítima);
   - Importancia del bien en el ecosistema marítimo global;
   - Tipo de activo (físico, cibernético, usuario, procedimientos).
4) Identificar el panorama de amenazas y la superficie de ataque de cada activo.
5) Seleccionar y utilizar una metodología de evaluación de riesgos (por ejemplo, del inventario de ENISA)[54] y estimar los riesgos.
6) Adoptar medidas para proteger los activos utilizando listas de controles publicadas, por ejemplo, ISO 27002, NIST2020, SANS Top 20, CIS y las mejores prácticas, y elaborar el plan de tratamiento de riesgos (plan de contingencia).
7) Desarrollar la política de seguridad con normas que regulen cómo se gestionan, protegen y distribuyen los activos dentro de la organización, utilizando los esfuerzos existentes, por ejemplo, PBIP, directrices BIMCO o ISO/IEC PDTR 13335-1 (11/2001).
8) Identificar continuamente nuevas amenazas, incidentes, evaluar los riesgos, la propiedad de los activos de las ICI, la solidez de los controles y la gestión de los incidentes.

[54] (Inventory of Risk Management / Risk Assessment Methods and Tools , n.d.)

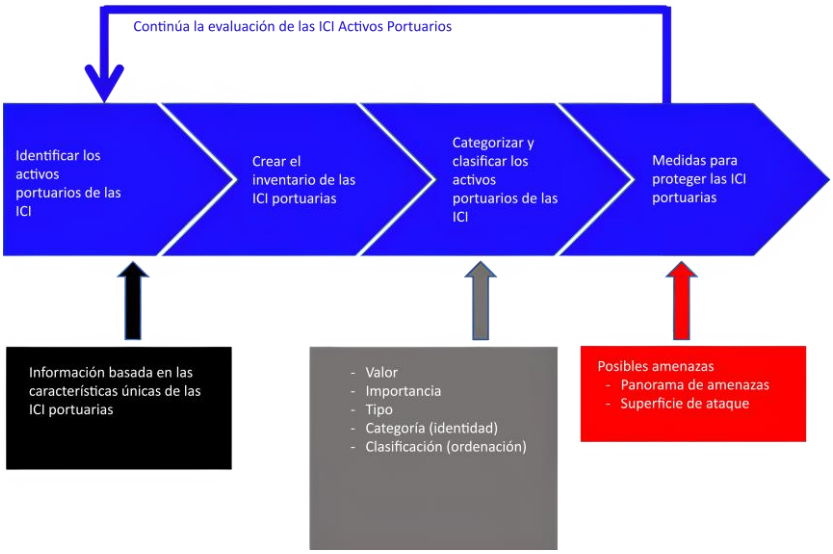


Figura 9: Enfoque BIMCO de la gestión de la seguridad

6.4.1 Gestión de la seguridad física

Antes del incidente del 11-S, los buques mercantes entraban tradicionalmente en aguas territoriales y puertos sin inspección para facilitar un comercio económico fluido y evitar retrasos de los buques. Sólo cuando el barco estaba anclado o amarrado subían a bordo las autoridades portuarias y los funcionarios de aduanas e inmigración para dar el visto bueno al barco, la tripulación y la carga. Esto hacía que el puerto fuera muy vulnerable a los ataques de organizaciones delictivas y terroristas. Un atentado terrorista contra un puerto podría afectar gravemente a las poblaciones locales, a las infraestructuras portuarias y a las economías regionales que dependen de estas actividades portuarias.

Las normas y protocolos de gestión de la seguridad portuaria también ayudan a prevenir accidentes y, por tanto, a reducir la gravedad de las lesiones si se produce un accidente. Es esencial porque crea un entorno de trabajo libre de peligros y riesgos mínimos. Esto mejora la calidad de las operaciones de la terminal y la reputación del puerto y puede considerarse una herramienta comercial para atraer más buques.

La OMI fue elegida como la organización más lógica para redactar un nuevo código de seguridad con entrada en vigor el 1 de julio de 2004, el Código PBIP. Inicialmente centrada en la gestión de la seguridad física (protección), ahora hace cada vez más hincapié en los riesgos de ciberseguridad y, en el futuro, se centrará también en los riesgos aéreos (es decir, ataques con drones).

Sin embargo, en algunos puertos marítimos sigue habiendo problemas de seguridad, lo que permite la entrada de amenazas para la seguridad en el puerto y sus instalaciones. Esto se debe en parte a que el Código PBIP nacional aplicado aborda las medidas de seguridad que deben adoptarse en las instalaciones portuarias y no como tales en la zona portuaria que rodea a estas terminales o en los socios comerciales/instalaciones de la cadena de suministro de los puertos.

Un puerto marítimo es un centro logístico e industrial de la cadena mundial de suministro económico. Las actividades portuarias, como el almacenamiento y la manipulación de buques, están directa o indirectamente relacionadas con el transporte internacional y los procesos de información en los que intervienen numerosos agentes. Esto significa que muchas personas entran y salen de los accesos portuarios a través de buques, camiones, ferrocarril, vehículos o como peatones. El CBP y el Código PBIP exigen que se controlen todos estos movimientos para evitar actos ilegales. El objetivo de esta sección no es explicar el Código PBIP en su totalidad ni todos los detalles del Código de Prácticas sobre Protección Portuaria, sino comprender cómo pueden aplicarse estos códigos en los puertos para resistir mejor los ataques. Todas las medidas de seguridad y prácticas operativas diarias que se describen a continuación se describen con más detalle en el PPP y el PPIP.

6.4.1.1 Límites del puerto y de las instalaciones portuarias

Ambos códigos exigen que se controle a todas las personas al entrar y salir del puerto o de una instalación portuaria. Pero, ¿cuáles son los límites administrativos de la instalación y, sobre todo, del puerto que hay que vigilar?

Las observaciones demuestran que, en algunos puertos, los capitanes no están seguros de ser la persona a la que hay que pedir cuentas y el responsable final como autoridad portuaria para actuar en caso de incidentes que ocurren a 90 millas mar adentro, o en la bahía del puerto o en un tramo de playa cercano fuera de la zona portuaria visual. Observamos confusión entre la autoridad portuaria y los operadores de las terminales privadas a la hora de determinar quién es responsable de los incidentes que se produzcan dentro del agua del muelle, frente a la respectiva instalación portuaria. Es importante incluir los límites administrativos exactos del puerto y de cada instalación portuaria (incluidos los límites marítimos) en el Plan de protección portuaria (PPP) y en el Plan de protección de la instalación portuaria (PPIP). Esto permite actuar con la mayor eficacia y ponerse en contacto con las personas adecuadas en caso de emergencia. Unas medidas eficaces evitan los daños consiguientes y garantizan el rápido restablecimiento de unas condiciones económicas normales.

6.4.1.2 Responsabilidad en materia de seguridad

Las instalaciones portuarias son las responsables últimas de la gestión de los incidentes de protección PBIP. Esto significa que el Oficial de Protección de la Instalación Portuaria (OPIP) debe actuar conforme a la normativa PBIP y el Oficial de Protección Portuaria (OPP) debe actuar conforme a las directrices del CBP. No corresponde al OPP asumir la responsabilidad global de los riesgos que se produzcan en las instalaciones portuarias, sino cooperar con la OPIP en ese caso.

La experiencia demuestra que en algunos países el Código PBIP se ha traducido en una ley nacional de seguridad que designa al OPP como responsable último de los incidentes de seguridad. Esto coloca a la OPP en una situación en la que el puerto (en lugar de la instalación portuaria) se convierte en la parte responsable final de los incidentes de protección PBIP en las instalaciones portuarias. El resultado es que los riesgos de protección quedan sin resolver porque es poco probable que el puerto invierta en medidas de protección dentro de una concesión de instalación portuaria privada.

6.4.1.3 El Sistema de Gestión de la Seguridad (SGS)

Para demostrar una gobernanza adecuada, los departamentos de protección portuaria deben estar bien organizados y tener en cuenta tanto las amenazas físicas como las cibernéticas. Deben ser capaces de supervisar y corregir las actividades diarias de seguridad y necesitan herramientas de gestión para ello. Con un sistema de gestión, pueden supervisar el estado de la infraestructura de seguridad y el rendimiento del personal de seguridad y verificar que todas las funciones de seguridad se realizan correctamente.

En muchos puertos no se dispone de SGS. Los responsables de seguridad actúan a veces como gestores de crisis y se centran en mitigar los incidentes en lugar de prevenirlos. Deben gestionar todos los aspectos de la seguridad y tomar medidas diarias para prevenir incidentes físicos, cibernéticos e híbridos. El Sistema de Gestión de la Seguridad de la Información (SGSI), que forma parte del SGS, se aplica mediante el cumplimiento de los requisitos de la norma ISO 27001.[55] Todas las IC del puerto deben cumplir los requisitos de la norma IS0 27001 y gestionar los ciberriesgos.

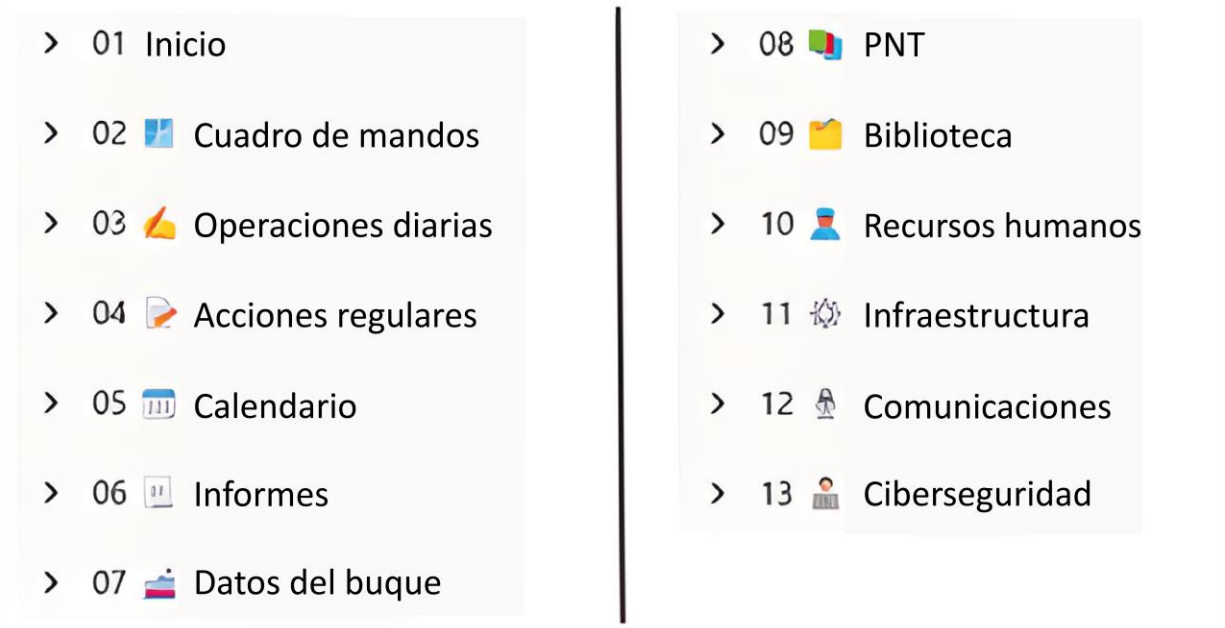


Imagen: Ejemplo de SGS (Christophe Van Maele)

6.4.1.4 Actividades de control de la seguridad física en las puertas

Cada vez que una persona (a pie o en un vehículo) entre en las instalaciones de PBIP, deberá comprobarse su tarjeta de identificación (o placa) antes de admitirla en la zona. El código exige un registro de la persona y la hora de entrada. Una vez que la persona abandona la instalación de PBIP, debe registrarse la hora de salida. Esto permite saber en todo momento quién se encuentra en la zona de PBIP y puede ayudar en la búsqueda de una persona concreta o durante una evacuación de emergencia. La tecnología puede ser de gran ayuda, ya que las barreras electrónicas, los torniquetes y los sistemas digitales de acreditación

[55] (ISO/IEC 27001 and related standards: Information security management, n.d.)

eliminan los registros manuales propensos a errores, sobre todo si el centro tiene varias entradas y salidas.

La realidad demuestra que el registro manual sigue siendo la norma en muchos puertos. Además, en el caso de barreras accionadas manualmente, el acceso es concedido por un vigilante, que puede decidir sin que se revise su decisión.

Si el puerto actúa como primer punto de entrada, lo que suele ocurrir cuando la zona portuaria es una zona franca, deben aplicarse los mismos principios de control de seguridad. Una vez más, en la práctica se observan muchas deficiencias.

6.4.1.5 Actividades de control de la seguridad en la zona portuaria

Los guardias de seguridad móviles realizan patrullas y comprueban que se permite la entrada a la zona PBIP o a la zona portuaria. Para facilitar esta tarea, todas las personas que se encuentren en la zona deberán llevar una tarjeta de identificación visible.
Sin embargo, rara vez se realizan controles de identificación, ni todas las personas llevan visiblemente su tarjeta de identificación.

6.4.1.6 Control de seguridad perimetral

El control perimetral es el control en los límites administrativos del puerto o de la instalación portuaria. En la mayoría de los casos existen barreras físicas, pero en la Unión Europea algunas terminales no críticas, como las de carga general que manipulan arena, no están obligadas a estar valladas. Es posible que dispongan de un sistema de cámaras para vigilar sus límites. La vigilancia del perímetro suele realizarse desde un Centro de Control de Seguridad, donde los operadores analizan las imágenes y deciden qué medidas tomar. Sus colegas de los equipos móviles de vigilancia hacen rondas de seguridad física. Es una buena práctica utilizar un sistema de rondas de vigilancia para asegurarse de que se han comprobado todas las zonas de puntos clave. A veces no se realizan rondas de vigilancia, y los operarios podrían estar mejor formados en muchos puertos.

6.4.1.7 Comunicación entre todas las partes interesadas en la seguridad

Deben organizarse reuniones periódicas entre los OPIP y el OPP para ponerse al día mutuamente sobre la situación actual detallada de la protección en el puerto, debatir los riesgos potenciales, gestionar los incidentes y mantenerse al corriente de las novedades que se produzcan en el puerto. Los OPP deberían celebrar el mismo tipo de reuniones a nivel nacional (Comité Nacional de Protección Marítima) con otras partes interesadas, como la policía portuaria, las aduanas, la marina, las autoridades designadas y otras. En estas reuniones se debaten cuestiones de seguridad de interés nacional y se abordan situaciones agudas, como el paso al nivel de seguridad 2 o 3.

En algunos países, las distintas partes interesadas permanecen en su propio terreno y no se reúnen con regularidad o no se reúnen en absoluto. En este caso, a menudo no existe un plan de acción coordinado o sólo existe sobre el papel, lo que deja margen para que las actividades delictivas pasen desapercibidas.

6.4.1.8 Refuerzo de las capacidades mediante la formación del personal

Es vital contar con personal de seguridad bien formado que sepa hacer su trabajo. En los puertos, la gente cambia a veces de trabajo, por lo que se requieren sesiones periódicas de formación para los nuevos reclutas y ensayos de seguridad para el personal de seguridad. Además de la formación básica PBIP, la formación en el puesto de trabajo es igualmente importante para entender cómo manipular las aplicaciones de la sala de control, a menudo digitalizadas, y cómo actuar en caso de emergencia.

La formación se considera necesaria en todos los puertos del mundo. Es importante mantener un alto nivel de formación para evitar que el personal formado no pueda responder eficazmente a los incidentes.

6.4.1.9 Gestión de incidentes de seguridad

Cuando el puerto ha implantado unos principios de gestión de la protección adecuados, las instalaciones portuarias que cumplen las normas PBIP pueden considerarse protegidas contra acciones ilegales intencionadas. Esto incluye los mencionados principios preventivos adoptados para proteger a las personas de robos, vandalismo, terrorismo, ciberataques, violencia, drogas y otras amenazas. Es importante comprender que, tanto en la reglamentación como en la gestión cotidiana, el PBIP y el CBP se basan en la prevención. Esto significa que las medidas de protección portuaria se toman en previsión de posibles amenazas antes de que se produzcan. Estas medidas están concebidas para disuadir a los delincuentes y reducir la probabilidad de que se produzca un delito o acto de violencia. Las evaluaciones de seguridad PBIP obligatorias (proceso de evaluación de la privacidad y la seguridad (EPP)/evaluación de la seguridad de las instalaciones portuarias (EPIP)) y los planes de seguridad (PPP / PPIP) constituyen la base de este estado de cumplimiento.

No obstante, si se produce un incidente de seguridad, el papel que desempeña el puerto puede cambiar. El paso a un nivel de protección PBIP superior es decisión de la autoridad designada. En ese caso, se reúne un equipo estratégico de crisis y se llama a las fuerzas del orden para que se ocupen de la situación aguda; por lo general, el puerto no decide por sí mismo qué medidas de seguridad proactivas inmediatas adoptar. Las medidas a largo plazo son propuestas por el puerto (instalación), aprobadas por la autoridad designada, incluidas en el plan de protección portuaria (instalación), y sólo entonces se aplican.

Los sistemas informáticos y de telecomunicaciones también se utilizan constantemente. En el ámbito de la protección de los puertos y las terminales que cumplen las normas PBIP, es necesario tener en cuenta lo siguiente:

- el sistema de gestión de la seguridad SGS sólo es eficaz si está digitalizado;
- el sistema de tarjetas identificativas es eficaz cuando se trata de un sistema digital basado en una base de datos común a la que también tienen acceso las fuerzas del orden y las aduanas;
- el sistema automático de barrera sólo admite a las personas con derecho a entrar en la zona;
- un sistema de vigilancia perimetral con un circuito cerrado de televisión de alto rendimiento u otro sistema de cámaras tomará medidas inteligentes y podrá realizar un seguimiento de las secuencias de vídeo durante largos periodos de tiempo;

- el uso de ordenadores para comunicarse entre las partes interesadas permite actuar en tiempo real y con eficacia cuando es necesario. Sin embargo, los sistemas de información siguen siendo competencia del departamento informático.

Hasta la fecha, varios de estos sistemas de seguridad no se han instalado en los puertos objeto del estudio. Por consiguiente, estos puertos no podrían ser atacados por ciberterroristas con respecto a estos sistemas. Este tipo de riesgo sólo se producirá cuando se digitalicen los sistemas de seguridad de estos puertos.

6.4.1.10 Control de los sistemas de información

Al digitalizarse cada vez más las operaciones cotidianas de seguridad, hay una gran cantidad de información que debe compartirse y protegerse. Esto se describe con más detalle en el capítulo sobre ciberseguridad.

6.4.1.11 Gestión de la seguridad de los buques

El Código PBIP se aplica a las instalaciones portuarias y a bordo de los buques. Aunque el mismo código se aplica a ambas zonas, hay varios aspectos que sólo se aplican a bordo de un barco. Si un terrorista se hace con el control de un buque, la carga, la tripulación y el sistema de información, podría paralizar un puerto durante mucho tiempo. El Oficial de Protección del Buque (SSO) es responsable de la correcta gestión de la protección a bordo, de conformidad con el Código PBIP, para prevenir los ataques piratas y los secuestros de buques. Están supervisados por su Responsable de Seguridad de la Compañía (CSO). Los principios de gestión corresponden a los del puerto.

Para estar preparados ante amenazas externas, la OMI ha tomado la iniciativa de ayudar a los buques con directrices para prevenir ataques. Un buque debe ser capaz de resistir un ataque externo mediante directrices de protección del buque. La aplicación de estas medidas de protección se divide en un primer nivel de defensa, un segundo nivel de protección y una capa final.

- El primer nivel de defensa protege al buque de ser abordada por atacantes. Esto incluye equipos de vigilancia, reflectores, maniobras para alejar el barco de los atacantes, alambre de espino y aspersores de agua y, en algunos casos, guardias armados privados.
- El segundo nivel de defensa tiene efecto una vez que los atacantes están a bordo y está diseñado para proteger el puente y el acceso al castillo. Esto puede hacerse mediante cerraduras de puertas, sensores de movimiento, sistemas de CCTV y un equipo de vigilancia.
- El tercer nivel de defensa se activa si los atacantes toman el puente y acceden al sistema de información. En ese caso, la tripulación puede esconderse en un búnker construido a tal efecto llamado Ciudadela, donde se dispone de los controles vitales del motor y la dirección, y se puede supervisar el sistema de comunicaciones.

La tripulación debe comprender perfectamente cómo funciona todo en la Ciudadela y cuáles son los medios importantes para mantener el control del buque desde allí. Si no están debidamente entrenados para controlar la nave desde este espacio búnker, la propia

Ciudadela puede convertirse en una prisión fatal para la tripulación reunida allí para su propia protección.

6.4.2 Gestión de la ciberseguridad

El modelo de gestión de la ciberseguridad desarrollado por BIMCO[56] (basado en el Marco de Gestión de Riesgos (RMF) del NIST)[57] sigue los pasos generales de evaluación de la seguridad descritos en la sección 6.4 y contiene los siguientes componentes relativos a la gestión del ciberriesgo:

1. Identificar las amenazas
2. Identificar vulnerabilidades
3. Evaluar la exposición al riesgo (estimación del riesgo)
4. Desarrollar medidas de protección y detección
5. Establecer planes de contingencia
6. Responder a incidentes de ciberseguridad y recuperarse de ellos

El punto más crucial a la hora de abordar la ciberseguridad es identificar el panorama de amenazas, lo que en la práctica significa identificar cuáles son las posibles amenazas que pueden afectar a los activos marítimos de IC. Algunos ejemplos de ciberamenazas identificadas durante el año 2020 por ENISA[58] son: (1) Malware, (2) Ataques basados en web (3) Phishing, (4) Ataques a aplicaciones web, (5) Spam, (6) DDoS, (7) Robo de identidad, (8) Violación de datos, (9) Amenaza interna, (10) Botnets, (11) Manipulación física, daños, robo y pérdida, (12) Fuga de información, (13) Ransomware, (14) Ciberespionaje, (15) Crypto jacking.

Tan pronto como se identifique el panorama de amenazas, se podrá identificar fácilmente la superficie de ataque -el conjunto de todos los ataques que se pueden utilizar para explotar las amenazas- de los activos de IC (punto 4 del apartado 6.4 anterior). La superficie de ataque de estos activos puede deducirse a partir de sus vulnerabilidades, por lo que es necesario realizar una evaluación de las mismas.

El siguiente paso identificado en BIMCO es evaluar la exposición al riesgo en relación con los activos de IC. En concreto, el riesgo se divide en cuatro tipos de respuesta al riesgo, a saber:

- *evitar el riesgo*: en este caso no se acepta el riesgo (es necesario que la alta dirección del puerto tome una decisión previa recomendación del Director de Seguridad de la Información (CISO))
- *transferir el riesgo* (es decir, a una compañía de seguros): una decisión de la alta dirección del puerto también debe tomarse por recomendación del CISO ya que podría tener repercusiones financieras.
- *Tomar medidas de mitigación*: mitigar el riesgo también es una decisión que debe

[56] (The Guidelines on Cyber Security onboard Ships - Version 4, 2020)
[57] (NIST Risk Management Framework (RMF), n.d.)
[58] (European Union Agency for Cybersecurity (ENISA), 2020)

tomar la alta dirección del puerto por recomendación del CISO, ya que también podría tener un impacto financiero.

- *se acepta* el riesgo: la aceptación del riesgo es una decisión empresarial directa y sólo la alta dirección puede tomar esta decisión.

Para mitigar el riesgo, hay que desarrollar medidas de protección y detección y establecer un plan de respuesta para llevar el riesgo a un nivel aceptable. El nivel aceptable lo define la IC marítima **(apetito de riesgo)** tras realizar un análisis coste-beneficio o tras identificar el impacto empresarial del riesgo. La **matriz de apetito por el riesgo** describe un análisis cualitativo del riesgo:

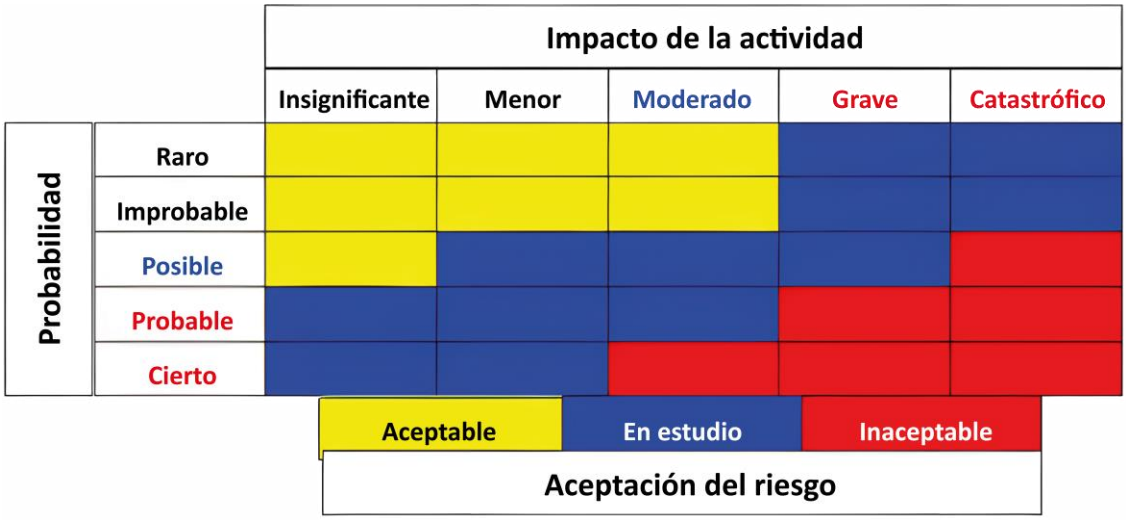


Figura 10: Matriz de apetito de riesgo

Si las medidas de mitigación no pueden llevar el riesgo a un nivel aceptable de acuerdo con la matriz de apetito de riesgo, entonces la alta dirección del puerto debe tomar una decisión empresarial para aceptar o no el riesgo.

Los riesgos deben evaluarse caso por caso en función del ecosistema cibernético de la IC y, en consecuencia, deben definirse como (i) aceptables, (ii) riesgos a debatir (medidas paliativas o riesgo transferido), o (iii) inaceptables, deben evitarse.

Las directrices de BIMCO sobre ciberseguridad a bordo de los buques se basan en principios de alto nivel:

- concienciación sobre los riesgos de seguridad, protección y comerciales que se presentan debido a la falta de medidas de ciberseguridad;
- protección de la infraestructura informática de a bordo y de los equipos conectados;
- sistema de autenticación y autorización de usuarios, para garantizar un acceso adecuado a la información necesaria;
- protección de los datos que se utilizan en el entorno de los buques, garantizando que cuentan con la protección adecuada en función de la sensibilidad de la información.

Figura 11: Enfoque de gestión de la ciberseguridad de BIMCO[59]

- gestión de los usuarios de TI, para garantizar que sólo tienen acceso y derechos a la información para la que están autorizados
- gestión de la comunicación entre el buque y la costa, y
- desarrollo y aplicación de un plan de respuesta a incidentes cibernéticos basado en una evaluación de riesgos.

El valor patrimonial de los puertos (importancia en las operaciones marítimas) determina los requisitos y controles de seguridad que deben llevarse a cabo. Diversos esfuerzos (por ejemplo, el proyecto SAURON) contribuyen a clasificar los activos portuarios y proponer arquitecturas de seguridad.

[59] (Directrices sobre ciberseguridad a bordo de los buques - Versión 4, 2020)

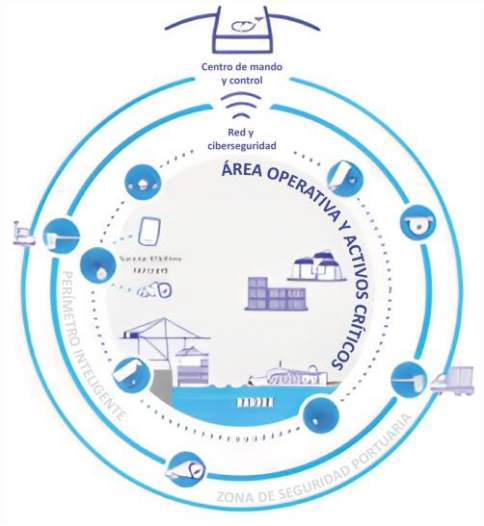


Figura 12: Arquitectura de seguridad física y cibernética SAURON[60]

Este enfoque contribuye a la seguridad de los puertos garantizando la seguridad de los activos físicos y la ciberseguridad de los activos cibernéticos.

6.5 Ciberresiliencia marítima

Ciberresiliencia marítima[61] es la capacidad de la IC marítima para resistir los ataques. La resiliencia se consigue si se garantiza la protección (seguridad y ciberseguridad) y si la estructura de gobernanza es eficaz y auditable, por ejemplo, si se comprueba periódicamente la solidez de los controles y procedimientos de seguridad (como los procedimientos de recuperación en caso de catástrofe).

Figura 13: Resiliencia marítima

[60] (Company, 2017); (Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports, n.d.)
[61] (Erstad, Ostnes, & Lund, 2021)

Diversas organizaciones adoptan una visión más general de la seguridad. Por ejemplo, según la Institution of Engineering and Technology (IET)[62], la seguridad se esfuerza por alcanzar y mantener ocho objetivos generales de seguridad, como se muestra a continuación:

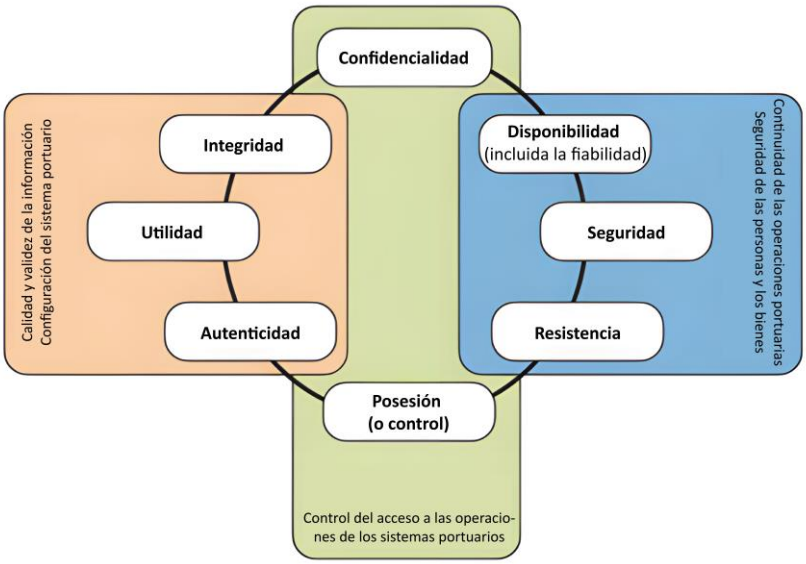


Figura 14: Objetivos de seguridad de la IET

6.6 Factores humanos

La naturaleza humana, el comportamiento, los valores sociales, culturales y éticos hacen que el individuo sea el principal facilitador de los ataques a la ciberseguridad o un hábil defensor de la ciberseguridad o un operador y oficial marítimo consciente de la seguridad. Los perfiles humanos y sus características desempeñan un papel fundamental en los futuros avances en la seguridad de los activos e infraestructuras marítimas.

La investigación de los factores y parámetros humanos de los miembros de los equipos de protección de puertos y buques o el estudio de los perfiles de los atacantes (a partir de incidentes de protección pasados) ayudan a prever o prevenir un incidente y a gestionar más eficazmente un ataque.

Además, al identificar los perfiles del personal marítimo (por ejemplo, operadores, agentes, administradores, miembros de la tripulación), la IC marítima puede desarrollar una formación en seguridad más eficaz que responda a sus necesidades y a sus niveles de comprensión de la seguridad. Los planes y procedimientos de seguridad deben ser claros para que todos los empleados puedan utilizarlos y adoptarlos a diario[63]. El desarrollo de procedimientos de seguridad aplicables requiere la participación de los empleados en la elaboración de dichos procedimientos.

[62] (Good Practice Guide: Cyber Security for Ports and Port Systems, 2020)
[63] (Kioskli & Polemi, Psychosocial Approach to Cyber Threat Intelligence, 2020); (Kioskli & Polemi, A Socio-Technical Approach to Cyber-Risk Assessment, 2020)

El factor humano es el punto de inflexión en la seguridad global del ecosistema marítimo. Normalmente, los puertos y los buques son los eslabones más débiles de la cadena de seguridad, lo que compromete las operaciones y los servicios marítimos a pesar de los medios tecnológicos existentes; las personas son la mayor amenaza.

La concienciación de las partes interesadas en la seguridad marítima debe ser objeto de un seguimiento continuo; la distribución y el análisis de los cuestionarios que figuran en el anexo pueden contribuir a esta necesidad. Las campañas de concienciación y la formación práctica específica son los medios para preparar a los empleados marítimos y a las partes interesadas para que se conviertan en los principales guardianes y defensores de la seguridad frente a los ataques físicos y cibernéticos en el ecosistema marítimo y mejoren la cultura marítima de la seguridad.

7 Prácticas de seguridad portuaria en África

7.1 Los puertos del Golfo de Guinea

Alrededor de 1500 buques al día (petroleros, cargueros y pesqueros) navegan por las aguas del Golfo de Guinea dirigiéndose a 20 grandes puertos. Este importante flujo económico crea una oportunidad de oro para la piratería y el secuestro de marinos, el robo a mano armada en el mar, la pesca ilegal, el contrabando y la trata de seres humanos en los puertos y sus alrededores, así como para la delincuencia organizada transnacional y los atentados terroristas. Supone una grave amenaza para la seguridad marítima de todos los buques que acuden a estos puertos y, en última instancia, para el desarrollo económico de los países de toda la región.

Se espera que el potencial económico de la región del Golfo de Guinea aumente aún más en los próximos años, pero antes de que pueda realizar y beneficiarse de este potencial, primero hay que hacer frente a las amenazas a su estabilidad y prosperidad. Para ello es necesario identificar y abordar continuamente los retos de seguridad relacionados con el mar, los puertos marítimos y el interior.

Figura 15: Región marítima del Golfo de Guinea[64]

7.2 Organización de la seguridad portuaria en África

Los puertos marítimos de África están organizados de la misma manera que los demás puertos del mundo. La autoridad portuaria está dirigida en sus operaciones cotidianas por funcionarios estatales, que responden ante sus respectivos ministerios.

Una Autoridad Portuaria tiene varios departamentos. Uno de los departamentos es el de Informática y otro el de Operaciones, dirigido por el Capitán del Puerto. Las observaciones realizadas en puertos de todo el mundo han demostrado que el Capitán del Puerto es el responsable general, aparte de las operaciones náuticas, de la seguridad dentro del puerto y

[64] (Gulf of Guinea Map, 2021)

de las instalaciones explotadas por el propio puerto. El departamento de protección debe aplicar la normativa PBIP en el puerto y hacer cumplir el escudo de protección. El departamento de seguridad portuaria, por su parte, se centra en la seguridad humana y casi siempre mantiene un equipo de intervención que actúa en caso de incendio y primeros auxilios. A nivel administrativo, el departamento de TI del puerto proporciona normas de ciberseguridad relacionadas con los sistemas administrativos generales del puerto, pero la infraestructura de seguridad del PBIP queda a menudo fuera de su ámbito y corre a cargo de las empresas externas que instalaron el hardware de seguridad. Los puertos reciben ingresos basados en el volumen de carga de los buques de sus clientes navieros a través del "recargo PBIP". Esta tasa cubre el coste del conjunto de medidas destinadas a mejorar la protección PBIP de las instalaciones portuarias.

Un ejemplo de buena práctica de seguridad es la siguiente arquitectura informática:

Hay 4 sistemas principales de seguridad TO e TI que son cruciales para prevenir un incidente de seguridad. Si alguno de estos sistemas es atacado por un ciberataque, la integridad de la seguridad física del puerto se ve comprometida.

- El primer sistema es el de *las tarjetas de acceso TO*: Un sistema de tarjetas de identificación se basa en una base de datos digital de las personas que hacen negocios en el puerto. La base de datos está compuesta por personal portuario, trabajadores portuarios, camioneros, clientes y visitantes. Tras un control administrativo inicial de la persona (realizado por la policía) al solicitar una tarjeta de identificación, se le permite entrar en el puerto en determinados días y a determinadas horas. En el mejor de los casos, la base de datos es revisada regularmente por la policía, que puede bloquear a personas con intenciones nefastas. Una empresa de seguridad externa instalará un sistema de tarjetas de identificación y tendrá derechos de administrador para mantener el sistema de TO. El personal de seguridad portuaria fabrica y distribuye las tarjetas. Si se piratea el sistema de credenciales y se amplía el tiempo de acceso, un delincuente puede recibir una credencial portuaria y entrar en la zona portuaria sin ser detectado.
- El segundo sistema de seguridad es *el sistema de control de acceso TO*: Este sistema permite a las personas acceder al recinto portuario (y a las instalaciones portuarias) cuando muestran su tarjeta de identificación dentro del horario autorizado. El sistema de control de accesos accede a la base de datos de tarjetas identificativas y decide si abre portones, puertas, torniquetes, barreras de acceso, etc. El sistema de control de accesos suele instalarlo el mismo integrador de seguridad que el sistema de tarjetas de acceso. Si el sistema de control de acceso puede ser engañado por un ciberataque, los delincuentes (y su contrabando) tienen vía libre para entrar y salir del puerto.
- El tercer sistema es el *sistema de control perimetral TO*: Para controlar el perímetro del puerto, se necesitan vallas y un sistema de vigilancia para controlar las entradas ilegales. Hoy en día, en los puertos civiles y las instalaciones portuarias se utilizan sistemas de CCTV, así como sistemas de cámaras térmicas e infrarrojas, para comprobar la integridad de la valla. Además, se ha construido una sala de control de seguridad para vigilar y actuar en caso de intrusión y violación. Estos sistemas de cámaras son instalados por empresas externas especializadas que tienen derechos administrativos sobre el sistema. Las cámaras las maneja el personal de seguridad del

puerto. Si el sistema de cámaras fuera pirateado por un ciberataque, se podría engañar a los guardias y mostrarles imágenes falsas, lo que permitiría la entrada ilegal o el robo a través de las vallas perimetrales.

Figura 16: Sistema de control perimetral TO[65]

- El cuarto sistema es *el informático*: El sistema informático utilizado por el personal de seguridad consiste principalmente en un sistema de gestión de la seguridad SGS, documentos de oficina digitales, correo electrónico y conexión a Internet. Este sistema lo instala el departamento informático del puerto, que conserva el control administrativo del escudo de ciberseguridad. Si se atrae a los operadores a un ciberataque, utilizando una memoria USB infectada, por ejemplo, podría impedirse la comunicación entre los vigilantes de seguridad, lo que daría lugar a una situación de seguridad ciega.

En otros puertos del sur y el este de África se aplican los mismos principios de seguridad que en los puertos del Golfo de Guinea. Los operadores portuarios privados que poseen instalaciones portuarias en régimen de concesión se organizan para ser seguros y cumplir las normas PBIP.

Las autoridades portuarias se centran en mantener segura la zona portuaria común dentro de los límites administrativos del puerto. Toman medidas para proteger esta zona desde la zona de fondeo, las zonas de amarre, hasta los muelles del puerto y toda la zona portuaria (zonas privadas exclusivas).

7.3 Iniciativas internacionales para los puertos africanos

Existen varios proyectos centrados principalmente en la mejora de la seguridad en alta mar, la piratería, las acciones transfronterizas y las drogas:

- EE.UU. están presentes con su Programa americano del Mando de África (AFRICOM), centrado en las iniciativas de seguridad en alta mar de los buques de guerra y el apoyo a las armadas locales.
- Los países del Golfo de Guinea y sus alrededores firmaron el "Código de Conducta relativo a la represión de la piratería, el robo a mano armada contra los buques y las

[65] Foto tomada por Christophe Van Maele

actividades marítimas ilícitas en África Occidental y Central" (Código de Conducta de Yaundé). Esta arquitectura de Yaundé promueve la cooperación marítima regional y salvaguarda un entorno marítimo estable.

- Europa está presente con el programa de Rutas Marítimas Críticas (CMR). Un conjunto de proyectos centrados en el marco jurídico, las normas operativas, el intercambio de información, la formación y el desarrollo de capacidades.
- La Red Interregional del Golfo de Guinea (GoGIN) pretende mejorar el conocimiento del dominio marítimo dentro de la red regional de intercambio de información dentro de la arquitectura de Yaundé (YARIS).
- El apoyo a la Seguridad Marítima Integrada de África Occidental (SWAIMS) pretende mejorar los marcos de aplicación de la ley y de gobernanza.
- El Programa de Apoyo a la Implementación de la Estrategia de Seguridad Marítima en el África Central (PASSMAR) se centra en la cooperación marítima transfronteriza.
- El Proyecto de Cooperación Portuaria Marítima (SEACOP) pretende crear capacidades y reforzar la cooperación contra el tráfico ilícito marítimo.
- Organizaciones internacionales como Interpol y el Programa Mundial sobre Desarticulación de Redes Criminales (CRIMJUST) de la ONUDD se centran en las rutas del narcotráfico.

Es decisión exclusiva del país cómo abordar la seguridad y la ciberseguridad en los puertos, y la participación internacional debe contar con la aprobación nacional.

- West and Central Africa Port Security project (WeCAPS),[66] un proyecto del CMR en la región del Golfo de Guinea, tiene como objetivo mejorar la seguridad portuaria y cumplir el PBIP. Este proyecto analiza los riesgos en 10 puertos de la región del Golfo de Guinea y ejecuta acciones de seguridad relativas a la formación del personal, el asesoramiento de expertos y la implantación del SGS.
- La OMI[67] y la Guardia Costera de Estados Unidos (USCG)[68] desempeñan un papel importante en los puertos marítimos sujetos al PBIP y están presentes con varias actividades de formación, visitas de mejora y proyectos de asistencia en los puertos africanos.

7.4 Ciberriesgos en África

Con la creciente digitalización de la industria marítima y el aumento del poder de las herramientas a disposición de los ciberdelincuentes, ha aumentado el número de ciberataques, incluidos los ataques a buques, y la aproximación a los puertos marítimos. Aunque hasta la fecha la mayoría de los incidentes de ciberseguridad marítima no han tenido como objetivo los puertos africanos, las pruebas disponibles de ciberataques en otros sectores y puertos de otras partes del mundo ayudan a proporcionar información valiosa a los gobiernos y autoridades portuarias africanos.

Estos ciberataques supondrían una amenaza existencial para la economía del continente africano si los puertos fueran atacados. Un reciente informe del Instituto de Estudios de

[66] (WeCAPS, n.d.)
[67] (Our Work, n.d.)
[68] (Atlantic Area Units, n.d.)

Seguridad[69] sobre la ciberseguridad africana en el mundo marítimo muestra cómo la ciberseguridad se está convirtiendo rápidamente en un aspecto importante de las necesidades de seguridad marítima africana a medida que la digitalización se afianza en la industria marítima de África. Con los actuales cambios tecnológicos en los buques, los puertos africanos tendrán que aumentar su escudo de ciberseguridad para seguir siendo competitivos. Los puertos africanos tienen que pensar de forma diferente sobre las amenazas, los riesgos y las vulnerabilidades, así como sobre las acciones delictivas.

Los buques van a la cabeza en el tratamiento de las medidas de ciberseguridad y están obligados a incluirlas en su manual ISM, y la OMI y sus compañías de seguros les exigen que se tomen en serio la ciberseguridad. A diferencia de las iniciativas a bordo de los buques, en los puertos marítimos del África Subsahariana sigue habiendo problemas de seguridad y ciberseguridad para mejorar su escudo.

Un ciberataque digno de mención tuvo lugar en julio de 2021, cuando Transnet, una importante empresa portuaria sudafricana, que gestiona el 60% del tráfico de contenedores del país en el puerto de Durban (Sudáfrica), sufrió un ataque de ransomware. Esto causó trastornos masivos. Sus terminales de contenedores de Durban, Ngqura, Port Elizabeth y Ciudad del Cabo tuvieron que pasar al procesamiento manual de la carga hasta que se restablecieron los sistemas informáticos. El resultado fue una enorme congestión de más de 14 horas para que los camiones recogieran y descargaran los contenedores y la inevitable pérdida de ingresos para el operador de la terminal. El Instituto de Estudios de Seguridad predijo en el mismo informe que incidentes como el ataque a Transnet aumentarán en toda África Subsahariana, ya que los puertos marítimos son objetivos atractivos, aún vulnerables a los ciberataques. En este caso, la infraestructura de transporte, especialmente un puerto, es un objetivo lucrativo para los ciberdelincuentes u otros actores hostiles debido a la escala de las operaciones y el alto impacto mediático internacional.

Aunque los principales puertos del África Subsahariana cuentan con departamentos de sistemas informáticos, la aplicación y el cumplimiento de medidas concretas de ciberseguridad distan mucho de haberse logrado, y esta situación supone un claro riesgo para la seguridad. Los responsables portuarios comprenden que es necesario avanzar y muestran gran interés por mejorar el blindaje de ciberseguridad de sus operaciones y sistemas de seguridad, como los sistemas de circuito cerrado de televisión, los sistemas de tarjetas identificativas y los sistemas de control de acceso. Pero las mismas autoridades portuarias no tienen suficientes conocimientos para mejorar su resistencia cibernética y parece haber pocas campañas de concienciación dirigidas a los puertos por parte de los responsables políticos nacionales para reducir los riesgos cibernéticos. No se observan muchos protocolos cibernéticos en los departamentos de seguridad portuaria.[70]

Uno de los proyectos de la CE en el Golfo de Guinea (WeCAPS) ha tomado la iniciativa de garantizar que el personal portuario de distintos niveles sea consciente de las ciberamenazas y los riesgos asociados y pueda actuar en consecuencia. Se centra en la formación de

[69] (Reva, 2020)
[70] (Africa's Maritime Cyber Security Progress After the Transnet Attack, 2021)

sensibilización de los operadores y el personal y habría llevado a cabo más acciones de mejora en el ámbito de las infraestructuras (sistemas de acceso, sistemas de tarjetas de identificación, sistemas de circuito cerrado de televisión y sistemas de comunicación) si el tiempo del proyecto lo hubiera permitido. El apoyo de este proyecto es coherente con las mejores prácticas destacadas por otras iniciativas, en particular la publicación de las Directrices de ciberseguridad para puertos e instalaciones portuarias de la IAPH 2021 y las Directrices de gestión de riesgos cibernéticos marítimos de la OMI.

Además del enfoque ascendente de WeCAPS, los responsables portuarios acogerían con satisfacción una ley nacional de ciberresiliencia. La Unión Africana tuvo un comienzo positivo en 2014 con la adopción del Convenio sobre Ciberseguridad y Protección de Datos Personales (el Convenio de Malabo)[71] y podría ser el primer paso hacia esta legislación. Además, los países africanos y los operadores privados de terminales podrían adoptar conjuntamente las mejores prácticas para garantizar la seguridad de sus infraestructuras marítimas.

[71] (African Union Convention on Cyber Security and Personal Data Protection, 2014)

8 Conclusiones

Las ICI marítimas incluyen, entre otros, puertos, buques y empresas marítimas. Las ICI marítimas son seguras si sus activos físicos son seguros y sus activos cibernéticos son ciberseguros. Este estudio abarcaba todos los aspectos importantes para la seguridad de las ICI marítimas: jurídico y político, tecnológico, normas y directrices.

9 Recomendaciones

El objetivo de este estudio no es crear un manual de buenas prácticas, sino enumerar brevemente las cuestiones que deben abordarse para construir un ciberescudo de alto rendimiento. Las mejores prácticas que se mencionan a continuación ayudarán a los operadores de puertos y buques a cumplir los requisitos de gestión de riesgos de ciberseguridad de la OMI, mejorando la seguridad y la fiabilidad de las cadenas de suministro y el comercio internacionales.

9.1 Recomendaciones para los puertos del África Subsahariana

Como ha demostrado este informe, un enfoque holístico de la seguridad es esencial. Estas primeras recomendaciones se refieren a la seguridad física, que complementaría las recomendaciones para mejorar la ciberseguridad que se enumeran más adelante. Las recomendaciones que aquí se formulan se basan en observaciones realizadas en varios puertos del África Subsahariana, donde es posible mejorar el escudo de protección:

1. Apoyo internacional a los países africanos para optimizar su legislación nacional de protección marítima aplicable a las zonas jurídicas portuarias administrativas, mediante la evaluación de la normativa vigente en materia de policía portuaria y aduanas, la normativa nacional PBIP y de protección portuaria, y otras normativas nacionales.
2. Reforzar la capacidad del personal de seguridad a través de diversas iniciativas, como:
    - Formación de pilotos de drones (contra posibles ataques aéreos)
    - Formación de responsables de protección de instalaciones portuarias PBIP y formación de guardias de seguridad en cooperación con la OMI
    - Guardias de seguridad con perros de seguridad adiestrados (contra drogas, productos químicos, explosivos)
    - Formación del personal de seguridad en Sistemas de Gestión de la Seguridad SGS
    - Asesoramiento experto en la instalación de sistemas de control de accesos, sistemas de control perimetral y Centros de Control de Seguridad Portuaria
    - Formación de tripulaciones de embarcaciones neumáticas semirrígidas a la interceptación en zonas portuarias
    - Formación en vigilancia para las tripulaciones de embarcaciones ancladas con el fin de prevenir los ataques piratas
    - Formación de la policía portuaria sobre las tareas de protección portuaria y la normativa PBIP
    - Inspección y formación de auditores para las autoridades designadas y el control del Estado rector de puerto
    - Creación de comités de protección portuaria en los que participen agentes privados y gubernamentales
3. Suministrar equipos críticos para el personal de seguridad de los puertos y para los operadores de terminales privadas, que les permitan ejecutar sus tareas con eficacia, como por ejemplo
    - Drones para policías y personal de seguridad
    - Embarcaciones neumáticas rígidas para patrullas marítimas, guardias de seguridad y policías
    - Equipos de comunicación para el personal de seguridad en tierra y en el agua

- Equipos de inspección para guardias de seguridad en las entradas de los puertos
- Sistemas de acceso para patrullas móviles
- Escáneres de rayos X para inspeccionar la carga en las aduanas

4. Acompañar a las autoridades navales, policiales, portuarias y marítimas designadas en sus esfuerzos por mejorar los procedimientos operativos normalizados y la planificación de la respuesta de emergencia en las zonas portuarias marítimas, para mejorar la seguridad de los buques fondeados, los canales de acceso a los puertos y las dársenas portuarias.
5. Reforzar las relaciones entre los diferentes agentes portuarios de los distintos países mediante seminarios de intercambio de experiencias y talleres técnicos. Con la participación de Ministerios de Transporte y Seguridad Nacional, Autoridades Designadas, responsables de puertos, puertos europeos y de otros lugares, OMI, USCG, Comisión Europea, The Shipowners' Club - Protection and Indemnity (P&I) y otras organizaciones de seguros, compañías navieras y operadores privados de terminales activos en el continente.

9.2 Recomendaciones a las partes interesadas del sector marítimo africano

Los países africanos en general necesitan mejorar su legislación en materia de ciberseguridad, al igual que muchos otros países del mundo con fronteras marítimas. Aparte de las iniciativas de protección portuaria, se observa que varios puertos siguen enfrentándose a retos para conseguir que sus puertos sean altamente resilientes a los ataques contra la protección y la ciberseguridad. Por lo tanto, se necesitan iniciativas adicionales de protección portuaria que ayuden a los legisladores nacionales, las autoridades portuarias, los operadores de terminales privadas, las autoridades nacionales designadas, la policía, las empresas privadas de protección portuaria y otras partes interesadas en los puertos y sus alrededores. Es muy recomendable reforzar estas iniciativas de PBIP junto con las de ciberseguridad en el ámbito jurídico-administrativo portuario (en tierra y en el agua). Estas iniciativas crearían un marco operativo mediante la capacitación, el apoyo al desarrollo de infraestructuras y equipos adecuados, la formación y el entrenamiento, y la ampliación de las asociaciones internacionales.

9.3 Apoyo de la alta dirección

La alta dirección es cada vez más consciente de las amenazas y riesgos cibernéticos y de su impacto potencialmente devastador en las operaciones de buques y puertos. La necesaria inversión continua en ciberseguridad se centrará específicamente en el personal de ciberseguridad, la gestión de la seguridad, los procesos y las tecnologías. Esto requiere la asignación de presupuesto y recursos y debe ser aprobado y apoyado por la alta dirección. Los riesgos cibernéticos afectan y pueden afectar a todos los que se encuentran en los puertos y buques. Por lo tanto, las medidas de ciberseguridad no deben ser responsabilidad exclusiva del departamento informático.

9.4 Formación en ciberseguridad

Todas las personas a bordo de un buque o en un puerto deben ser conscientes de las amenazas y de cómo les afectan los incidentes cibernéticos. Por lo tanto, deben recibir formación sobre ciberseguridad para saber qué pueden hacer para garantizar que el puerto y el buque sigan siendo seguros. La formación debe adaptarse por funciones.

9.5 Procedimientos, directrices e instrucciones de ciberseguridad

El personal de puertos y buques debe saber exactamente qué se espera de ellos y cómo gestionar la ciberseguridad. Deben recibir Procedimientos Normalizados de Trabajo (PNT) sobre cómo gestionar sus tareas diarias, así como la gestión de incidentes. Deben formarse equipos de ciberseguridad, celebrar reuniones periódicas y tener un impacto en las operaciones.

9.6 Servicios y funciones críticos de la organización

Para saber cómo abordar la ciberseguridad, es vital conocer qué sistemas existen en el puerto y a bordo de los buques. Un inventario debe incluir todos los activos físicos y cibernéticos críticos, incluidos dispositivos, sistemas, software y aplicaciones tanto de TI como de TO.

9.7 Evaluación de los riesgos de ciberseguridad

Con el inventario en la mano, se debe llevar a cabo una evaluación de riesgos para identificar las amenazas, los riesgos y las vulnerabilidades relacionadas con los activos de TI y TO que podrían afectar negativamente a las operaciones y la seguridad.

9.8 Plan de gestión de la ciberseguridad

Además de los planes de protección portuaria PBIB (instalaciones) y de los planes de protección de los buques existentes, debe elaborarse un plan de gestión de la ciberseguridad, ya que estos planes se centran principalmente en la protección física. Este plan incluirá medidas para hacer frente a los riesgos identificados sobre la base de la evaluación de riesgos, responsabilidades de ciberseguridad de la tripulación, procedimientos para responder a las amenazas de ciberseguridad y procedimientos para auditar las actividades de ciberseguridad. El plan incluiría medidas tanto técnicas como de procedimiento para minimizar los riesgos cibernéticos.

9.9 Ciberseguridad de la cadena de suministro

Los proveedores de equipos pueden tener acceso remoto a sistemas críticos a bordo (por ejemplo, sistemas de navegación, sistemas de alimentación de motores, sistemas de carga, etc.) o en las instalaciones portuarias (por ejemplo, esparcidores de contenedores, grúas portuarias, sistemas grúas pórtico montadas sobre rieles (RMG), y grúas pórtico montadas sobre neumáticos (RTG), etc.), y cualquier incidente de ciberseguridad en el lado del proveedor puede afectar al buque o a los equipos y sistemas de manipulación específicos de los que son responsables. Por lo tanto, es importante evaluar la ciberseguridad de los proveedores para identificar riesgos en sus servicios y sistemas que puedan afectar negativamente al funcionamiento de los buques y puertos.

9.10 Gestión de incidentes, respuesta y recuperación

Los buques y puertos deben aplicar políticas, procedimientos y controles adecuados que les permitan detectar, responder, recuperarse, y aprender de los incidentes de ciberseguridad.

9.11 Normas y marcos de ciberseguridad

No es fácil gestionar todos los aspectos de la gestión de la ciberseguridad sin recurrir a la ayuda y orientación de las normas y directrices existentes. Por lo tanto, la gestión de la ciberseguridad debe utilizar políticas, procesos y procedimientos sobre controles técnicos y concienciación de los empleados para gestionar la ciberseguridad en los puertos y a bordo de

los buques. El asesoramiento experto de consultores marítimos que puedan ayudar a implantar la ciberseguridad en el entorno portuario y naval es importante para evitar errores.

9.12 Recomendaciones generales sobre ciberseguridad portuaria

Las recomendaciones de ciberseguridad que se enumeran a continuación para su aplicación en los puertos marítimos supondrían una diferencia positiva en materia de ciberseguridad para las autoridades portuarias y otras partes interesadas que trabajan en el puerto.

1. Legislación portuaria sobre ciberseguridad

Aplicar/ajustar la legislación nacional para que cumpla la legislación, códigos y directrices internacionales sobre ciberseguridad portuaria, ya que es el motor del comercio internacional fiable.

2. Evaluación de la ciberseguridad (CSA)

De conformidad con las normas de protección PBIP, se realizan evaluaciones de protección (EPP y EPIP) de los puertos y las instalaciones portuarias. El objetivo de estas evaluaciones es identificar los puntos vulnerables de las estructuras físicas, los sistemas de protección del personal y los procesos empresariales que podrían dar lugar a un incidente de seguridad. La evaluación de la ciberseguridad pretende basarse en las evaluaciones de seguridad PBIP existentes cuando proceda. Utilizar las normas existentes (por ejemplo, ISO270xx) y las mejores prácticas internacionales (por ejemplo, OMI/BIMCO, ENISA, IACS) para evaluar, estimar y mitigar los riesgos cibernéticos y físicos.

3. Plan de Ciberseguridad (CSP)

Las evaluaciones de protección constituyen la base de los planes de protección portuaria (PPP) y de los planes de protección de las instalaciones portuarias (PPIP). Estos planes abordan los problemas identificados en la evaluación pertinente estableciendo medidas de seguridad apropiadas diseñadas para minimizar la probabilidad de una violación de la seguridad y las consecuencias de los riesgos potenciales. El plan de ciberseguridad debe basarse en el PPP o PPIP existente cuando proceda. También es importante poner a prueba el plan, preferiblemente con ejercicios de simulación, para garantizar que está actualizado y que todas las partes interesadas lo comprenden.

Un PCS tiene la misma función que el plan de protección PBIP para las cuestiones identificadas en la CSA, considerando también el impacto de las medidas establecidas en el PPP y el PPIP.

4. Organización cibernética

Para la gestión de la ciberseguridad, es vital disponer de un organigrama en el que se asignen funciones y tareas específicas a las distintas partes interesadas.

- El nombramiento de un Responsable de Ciberseguridad del buque (CySO), responsable de la ciberseguridad del puerto y de las instalaciones portuarias gestionadas por el puerto.
- Creación de un Comité de Protección Portuaria al que asistan las distintas partes interesadas.
- Creación de un Centro de Operaciones de Seguridad (COS).

5. Gestión de la ciberseguridad

Una vez establecido el escudo de ciberseguridad mediante la creación de la CSA y el PCS, es importante que el COS disponga de los mecanismos de gestión y funcionamiento adecuados, entre los que se incluyen:

- Auditoría y revisión periódicas del PCS
- Simulaciones periódicas de ciberataques
- Seguimiento de la evolución del ciberescudo
- Métodos para facilitar información a terceros
- Cómo gestionar los incidentes de seguridad
- Pruebas periódicas de los planes y de la gestión de incidentes mediante ejercicios teóricos.

6. Formación para el desarrollo de capacidades

Las personas trabajan con sistemas de TO e TI y necesitan formación periódica para trabajar con eficacia. Por lo tanto, la formación a distintos niveles es vital:

- Formación para el personal de seguridad (operadores), que utiliza a diario los sistemas TO y TI de seguridad.
- Formación para la gestión de la seguridad (OPIP, OPP), para comprender las consecuencias y el impacto en la seguridad de los sistemas de TI y TO. Deben ser capaces de minimizar los daños, aplicar contramedidas de seguridad inmediatas y volver a la situación normal lo antes posible.
- Formación del personal informático implicado en la seguridad de los sistemas TO. Deben ser capaces de instalar y mejorar el escudo de ciberseguridad para el personal de seguridad.

Las recomendaciones de seguridad anteriores se exponen en el siguiente cuadro:

Nº	Recomendaciones
1	Optimizar las leyes nacionales de protección marítima (reglamentos de policía portuaria y aduanas, reglamentos nacionales PBIP y de protección portuaria)
2	Formación de oficiales de protección de instalaciones portuarias PBIP y formación de guardias de seguridad en cooperación con la OMI
3	Formación de guardias de seguridad con perros y puertas inteligentes (contra drogas, productos químicos, etc.)
4	Formación del personal de seguridad en los sistemas de gestión de la seguridad SGS
5	Asesoramiento en la instalación de sistemas de control de accesos, sistemas de control perimetral y Centros de Control de Protección Portuaria
6	Formación de tripulaciones de embarcaciones neumáticas semirrígidas y de interceptación en zonas portuarias
7	Formación en vigilancia para las tripulaciones de embarcaciones ancladas con el fin de prevenir los ataques piratas
8	Formación de la policía portuaria sobre las tareas de protección portuaria y la normativa PBIP

9	Inspección y formación de auditores para las autoridades designadas y el control del Estado rector del puerto
10	Creación de comités de protección portuaria en los que participen agentes privados y gubernamentales
11	Suministrar equipos certificados de seguridad para el personal de seguridad de los puertos y para los operadores de terminales privadas (drones, embarcaciones neumáticas semirrígidas, equipos de comunicación, equipos de inspección, sistemas de acceso y escáneres de rayos X).
12	Acompañar a la fiscalía, la policía y la marina para mejorar los procedimientos operativos estándar y la planificación de la respuesta de emergencia (en tierra y en el agua).
13	Reforzar las relaciones entre los distintos agentes portuarios internacionales.
14	Mejorar la legislación, las prácticas y los procedimientos nacionales en materia de ciberseguridad portuaria
15	Evaluación y gestión de la ciberseguridad
16	Establecer, aplicar, auditar y mejorar continuamente el Plan de Ciberseguridad
17	Nombrar un responsable de ciberseguridad y un equipo de ciberseguridad
18	Crear un Comité de Protección Portuaria
19	Colaborar/establecer y operar un COS
20	Organizar un grupo de gestión diaria para tratar los incidentes y otras tareas cotidianas de ciberseguridad
21	Formación del personal de seguridad (operadores de seguridad)
22	Formación para la gestión de la seguridad (PFSO, PSO)
23	Formación del personal informático implicado en la seguridad de los sistemas TO

9.13 Recomendaciones a la UE: Hacia una colaboración estable UE-África

Una colaboración UE-África en los siguientes ámbitos mejoraría la seguridad marítima mundial y la seguridad de nuestras cadenas de suministro:

- *Establecer colaboraciones estables* entre Ministerios de Transporte Marítimo, Agencias de Seguridad e ISACS marítimos para llegar a un entendimiento común, realizar un seguimiento continuo, mitigar los retos de seguridad y los incidentes de seguridad transfronterizos en el ecosistema marítimo. Crear fuertes sinergias e intercambiar conocimientos, recomendaciones y buenas prácticas.
- *Campañas de sensibilización y formación sobre seguridad marítima*: Establecer una colaboración con entidades públicas y privadas para crear centros de sensibilización sobre seguridad marítima, formación operativa y formación sobre gestión de incidentes orientados a las necesidades generales de seguridad marítima y específica del transporte marítimo, en los que las plataformas de simulación y ejercicios facilitarían el desarrollo de capacidades.

- *Cerrar la brecha de habilidades cibernéticas* con evaluaciones de riesgo prácticas, simulación virtual de ataques industriales e incidentes dirigidos a la industria naviera, y el ecosistema digital marítimo general y de la cadena de suministro internacional. El uso extensivo de ciberespacios puede ayudar a las partes interesadas de la industria naval a mejorar su comprensión a la hora de gestionar ataques e incidentes complejos y mejorar la preparación y resiliencia del sector naval. Esto implicaría experimentos realistas basados en pruebas y ejercicios de "captura la bandera" con equipos de ciberseguridad y de ataque enfrentados entre sí. La Asociación Internacional de Sociedades de Clasificación (IACS) y la OMI pueden aprovechar la experiencia de ENISA-Cyber Europe y seguir colaborando con ENISA y CERT-EU para promover la formación en ciberseguridad y allanar el camino hacia una formación eficaz en el sector marítimo.
- *Apoyo transfronterizo en el funcionamiento de COS marítimos* que prevean y gestionen eficazmente los ciberataques y los incidentes de seguridad.
- *Armonizar los esfuerzos de certificación marítima*: Auditar y evaluar conjuntamente la seguridad de los equipos marítimos para garantizar la privacidad, la seguridad, la transparencia, la interoperabilidad, la rendición de cuentas, la responsabilidad y el cumplimiento de la legislación y las directrices de seguridad de la UE e internacionales. Animar a las comunidades de fabricantes, desarrolladores e integradores de la UE y África (militares y civiles) a adoptar la cultura de compartir responsabilidades en materia de seguridad mediante la realización de pruebas de conformidad comunes utilizando normas internacionales.
- *Realizar* periódicamente *análisis comparativos* entre puertos de la UE, de la región del África Subsahariana y puertos de otras regiones del mundo, como el Sudeste Asiático. Esto sería útil para destacar los enfoques de seguridad y ciberseguridad UE-África que han tenido éxito y que pueden reproducirse en otras regiones.

10 Referencias

Acharya, T. (2019, July 31). *Black boxes and their intrusion*. Retrieved from Towards Data Science: https://towardsdatascience.com/black-boxes-and-their-intrusion-620aa3c4c56b

Africa Maritime Technology Cooperation Centre launched in Mombasa. (2017, December 13). Retrieved from EEAS: https://www.eeas.europa.eu/node/37286_en

(2014). *African Union Convention on Cyber Security and Personal Data Protection.* African Union. Retrieved from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Africa's Maritime Cyber Security Progress After the Transnet Attack. (2021, September 16). Retrieved from The Maritime Executive: https://maritime-executive.com/article/africa-s-maritime-cyber-security-progress-after-transnet-attack

Alcaide, J. I., & Garcia-Llave, R. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia, 45*, 547-554. doi:10.1016/j.trpro.2020.03.058

Alderton, P. (1999). *Port Management and Operations.* LLP Professional Publishing. Retrieved from https://commons.wmu.se/cgi/viewcontent.cgi?article=1070&context=all_dissertations

Ashraf, I., Park, Y., Hur, S., Kim, S., Alroobaea, R., Bin Zikria, Y., & Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1-14. doi:10.1109/TITS.2022.3164678

Atlantic Area Units. (n.d.). Retrieved from United States Coast Guard Atlantic Area: https://www.atlanticarea.uscg.mil/Our-Organization/Area-Units/

Burt, J. (2021, August 10). Cybersecurity Landscape and Threats to Maritime Operations. Retrieved from https://www.tenntom.org/wp-content/uploads/2021/10/CISA-Jason-Burt_CISA_Cybersecurity-Port_Maritime-Security.pdf

China hackers steal data from US Navy contractor - reports. (2018, June 9). Retrieved from BBC: https://www.bbc.com/news/world-us-canada-44421785

Code of Safe Practice for Cargo Stowage and Securing (CSS Code). (n.d.). Retrieved from IMO: https://www.imo.org/en/OurWork/Safety/Pages/CSS-Code.aspx

Company, R. (2017, July 21). *How ports can protect themselves against cyber and physical security threats*. Retrieved from Medium: https://medium.com/@ICHCA/how-ports-can-protect-themselves-against-cyber-and-physical-security-threats-b6bd10c4f7a7

Costa Concordia: What happened. (2015, February 10). Retrieved from BBC: https://www.bbc.co.uk/news/world-europe-16563562

Coulibaly, S., Kassa, W., & Zeufack, A. (2022, June). *Re-engineering African trade with the European Union and United States: Success requires reform on both sides*. Retrieved from World Bank Blogs: https://blogs.worldbank.org/africacan/re-engineering-african-trade-european-union-and-united-states-success-requires-reform

Darbra, R.-M., & Casal, J. (2004, February). Historical analysis of accidents in seaports. *Safety Science, 42*(2), 85-98. doi:10.1016/S0925-7535(03)00002-X

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016). Retrieved from https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Drougkas, D. A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019, November 26). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector.* ENISA. Retrieved from ENISA: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

(2022). *ENISA Threat Landscape 2022.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Erstad, E., Ostnes, R., & Lund, M. (2021, March). An Operational Approach to Maritime Cyber Resilience. *TransNav, 15*(1). doi:10.12716/1001.15.01.01

ESPO: The First Port of Call for European Transport Policy Makers in Brussels. (n.d.). Retrieved from ESPO: https://www.espo.be/

EU-Africa: Global Gateway Investment Package. (n.d.). Retrieved from European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

European Maritime Safety Agency . (n.d.). Retrieved from AESM: https://www.emsa.europa.eu/

European Union Agency for Cybersecurity (ENISA). (2020). ENISA Threat Landscape: 15 Top Threats in 2020. Retrieved from https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

(2020). *Good Practice Guide: Cyber Security for Ports and Port Systems.* The Institution of Engineering and Technology. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf

Greater and More Diverse Participation in Global Trade is Key to Achieving Africa's Economic Transformation, says New World Bank Book. (2022, February 10). Retrieved from The World Bank: https://www.worldbank.org/en/news/press-release/2022/02/10/greater-and-more-diverse-participation-in-global-trade-is-key-to-achieving-africa-s-economic-transformation-says-new-wor

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Retrieved from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

(2020). *Guidelines - Cyber Risk Management for Ports.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

(2017). *Guidelines on Maritime Cyber Risk Management.* London: IMO. Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Gulf of Guinea Map. (2021). Retrieved from https://issafrica.s3.amazonaws.com/site/images/2021-02-10-gulf-of-guenea-piracy-map.png

Hand, M. (2020, April 17). *MSC confirms malware attack caused website outage*. Retrieved from Seatrade Maritime News: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Herald of Free Enterprise Ferry Disaster – 1987. (n.d.). Retrieved from Devastating Disasters: https://devastatingdisasters.com/herald-of-free-enterprise-ferry-disaster-1987/

ILO: International Labour Oeganization. (n.d.). Retrieved from UN: Office of the Secretary-General's Envoy on Youth: https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid=CjwKCAiAv9ucBhBXEiwA6N8nYF5eTI5UjefYhsbZBgjQa8jYr3hWW0MocPuYj4mAk-nPawYFcgjb1hoCS3QQAvD_BwE

International Convention for the Safety of Life at Sea (SOLAS), 1974. (n.d.). Retrieved from IMO: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 197. (n.d.). Retrieved from IMO: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx

Inventory of Risk Management / Risk Assessment Methods and Tools . (n.d.). Retrieved from European Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory

ISO/IEC 27001 and related standards: Information security management. (n.d.). Retrieved from ISO: https://www.iso.org/isoiec-27001-information-security.html

Jørgensen, R. N. (2018). *Cyber security survey shows more action is needed in the industry*. Retrieved from BiMCO: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Kalogeri, E., & Polemi, N. (2022). A taxonomy of maritime security standards. *6th NMIOTC Conference on Cyber Security in Maritime Domain.* Souda Bay: NATO.

Kioskli, K., & Polemi, N. (2020). A Socio-Technical Approach to Cyber-Risk Assessment. *International Journal of Electrical and Computer Engineering, 14*(10), 305-309. Retrieved from https://publications.waset.org/10011507/a-socio-technical-approach-to-cyber-risk-assessment

Kioskli, K., & Polemi, N. (2020). Psychosocial Approach to Cyber Threat Intelligence. *International Journal of Chaotic Computing, 7*(1), 159-165. doi:10.20533/ijcc.2046.3359.2020.0021

Langewiesche, W. (2004, May). A Sea Story. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2004/05/a-sea-story/302940/

Maritime trade and Africa. (2018, October 3). Retrieved from UNCTAD: https://unctad.org/press-material/maritime-trade-and-africa

(2021). *Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities.* IMO. Retrieved from https://events.iala-aism.org/content/uploads/2021/09/MSC-104-7-1-IAPH-Cybersecurity-Guidelines-for-Ports-and-Port-Facilities-IAPH.pdf

Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø., & Nesheim, D. (2021, September). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, 15*(3). doi:10.12716/1001.15.03.04

MTCC Africa. (n.d.). Retrieved from MTCC Africa: http://mtccafrica.jkuat.ac.ke/

Negreiro, M. (2022). *The NIS2 Diretive: A high common level of cybersecurity in the EU.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

NIST Risk Management Framework (RMF). (n.d.). Retrieved from NIST: Computer Security Resource Center: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/

Our Work. (n.d.). Retrieved from IMO: https://www.imo.org/en/OurWork/Pages/Default.aspx

Polemi, N. (2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains.* Elsevier. doi:9780128118191

Port of San Diego: phishing emails remain amongst greatest cyber threats. (2021, August 19). Retrieved from Port Technology International: https://www.porttechnology.org/news/port-of-san-diego-phishing-emails-remain-amongst-greatest-cyber-threats/#:~:text=The%20Port%20of%20San%20Diego%20reported%20a%20ransomware,hacker%20operating%20inside%20the%20Islamic%20Republic%20of%20Iran.

Resolution A.682 (17). (1991). International Maritime Organization. Retrieved from https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.682(17).pdf

Reva, D. (2020). *Maritime cyber security: Getting Africa ready.* Institute for Security Studies. Retrieved from https://issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf

(n.d.). *Rulebook 2021.* UKP&I. Retrieved from https://www.ukpandi.com/news-and-resources/rulebook-2021/

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports. (n.d.). Retrieved from CORDIS: https://cordis.europa.eu/project/id/740477

Shapira, I. (2006, January 4). Captain Blamed in Fatal Tanker Explosion Off Va. *The Washington Post*. Retrieved from https://www.washingtonpost.com/archive/local/2006/01/04/captain-blamed-in-fatal-tanker-explosion-off-va/f4a4ffc8-6cea-4893-ba6c-e9afd76eec8d/

SOLAS XI-2 and the ISPS Code. (n.d.). Retrieved from IMO: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Standards. (n.d.). Retrieved from ISO: https://www.iso.org/standards.html

(2018). *Strenghtening Africa's gateways to trade.* PwC. Retrieved from https://www.pwc.co.za/en/assets/pdf/strengthening-africas-gateways-to-trade.pdf

The Beirut Port Explosion. (n.d.). Retrieved from Forensic Architecture: https://forensic-architecture.org/investigation/beirut-port-explosion

(2020). *The Guidelines on Cyber Security onboard Ships - Version 4.* BIMCO. Retrieved from https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

The International Safety Management (ISM) Code. (n.d.). IMO. Retrieved from https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

(2021). *Threat Landscape for Supply Chain Attacks.* European Union Agency for Cybersecurity (ENISA). Retrieved from https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Titanic. (n.d.). Retrieved from Britannica: https://www.britannica.com/topic/Titanic/Aftermath-and-investigation#ref302525

Tomter, L., & Gundersen, M. (2019, April 14). *IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre*. Retrieved from NRK: https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_-man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043

WeCAPS. (n.d.). Retrieved from Strengthening the security and safety of ports in West and Central Africa : https://wecaps.eu/en/

Widup, S. (2019). *2019 Verizon Data Breach Investigations Report.* Verizon. Retrieved from https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

Winder, D. (2019, July). *U.S. Coast Guard Issues Alert After Ship Heading Into Port Of New York Hit By Cyberattack*. Retrieved from Forbes: https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=78d82cb141aa

11 Anexos: Cuestionarios de seguridad

11.1 Anexo A: Cuestionario de concienciación sobre gobernanza de la seguridad

Basándose en la norma ISO27001[72], el siguiente cuestionario puede servir para evaluar comparativamente la estructura de gobernanza de una empresa marítima para gestionar los riesgos de seguridad:

Objetivo de control	Tema	Pregunta	No	Sí
Política de protección (seguridad y ciberseguridad)	Política de seguridad de la información	¿Conoce el personal el vínculo de la política de seguridad con sus funciones?		
Organización de la seguridad	Organización interna	¿Es consciente el personal de sus responsabilidades en materia de seguridad?		
		¿Posee el personal las autorizaciones necesarias?		
	Partes externas	¿Es consciente el personal de los posibles riesgos al tratar con partes externas?		
		¿Toma el personal medidas de seguridad en el trato con los clientes?		
Gestión de activos	Responsabilidad de los activos	¿Es consciente el personal de los activos con los que trata?		
		¿Conoce el personal la propiedad de estos activos?		
		¿Conoce el personal el uso de los activos?		
	Clasificación de la información	¿Conoce el personal las directrices de clasificación?		
		¿Conoce el personal la información de acceso y manipulación?		
Seguridad de los recursos humanos	Durante el empleo	¿Conoce el personal sus responsabilidades de gestión?		
		¿Se ha formado al personal en temas de concienciación en materia de seguridad (por ejemplo, medidas de control de acceso) y ciberseguridad (por ejemplo,		

[72] De la Organización Internacional de Normalización (ISO); https://www.iso.org/isoiec-27001-information-security.html

		phishing, ingeniería social, almacenamiento de datos)?		
	Cese de la relación laboral	¿Sabe el personal que al cesar en su empleo tiene que devolver sus activos y se le retiran los derechos de acceso?		
Seguridad física y medioambiental	Zonas seguras	¿Conoce el personal el perímetro de seguridad física del puerto?		
		¿Conoce el personal los controles físicos de entrada?		
		¿Conoce el personal el procedimiento de seguridad del lugar de trabajo?		
	Seguridad de los equipos	¿Conoce el personal el uso de los equipos de seguridad e informáticos de los locales?		
		¿Conoce el personal la política de "trae tu propio dispositivo"?		
		¿Conoce el personal los procedimientos para la eliminación segura o la reutilización de equipos?		
Comunicaciones y gestión de operaciones	Procedimientos operativos y responsabilidades	¿Conoce el personal los procedimientos operativos relacionados con las actividades?		
		¿Conoce el personal el proceso de gestión del cambio?		
	Protección contra código malicioso y móvil	¿Conoce el personal los controles contra códigos maliciosos (por ejemplo, manipulación de correos electrónicos)?		
		¿Conoce el personal los controles contra el código móvil (es decir, los dispositivos móviles infectados)?		
	Copia de seguridad	¿Conoce el personal el proceso de copia de seguridad de la información?		
	Tratamiento de los medios de comunicación	¿Conoce el personal la gestión de los soportes extraíbles?		
		¿Sabe el personal cómo deshacerse de los soportes?		
		¿Conoce el personal los procedimientos de tratamiento de la información?		
		¿Es consciente el personal de la seguridad de la documentación del sistema?		

	Intercambio de información	¿Es consciente el personal de la protección de los soportes físicos en tránsito?		
		¿Conoce el personal la mensajería electrónica?		
	Servicios marítimos electrónicos	¿Conoce el personal el procedimiento sobre las transacciones en línea y el uso de la información disponible públicamente?		
	Supervisión	¿Conoce el personal la política relativa a los registros?		
Control de acceso	Requisitos empresariales para el control de acceso	¿Conoce el personal la política de control de acceso?		
	Gestión de acceso de usuarios	¿Conoce el personal el procedimiento de registro de usuarios?		
		¿Conoce el personal la política/gestión de contraseñas de los usuarios?		
		¿Conoce el personal el procedimiento de los derechos de acceso de los usuarios?		
	Responsabilidades del usuario	¿Es consciente el personal del uso de contraseñas?		
		¿Conoce el personal el procedimiento de equipos de usuario desatendidos?		
		¿Conoce el personal la política de escritorio limpio y pantalla despejada?		
	Control de acceso a la red	¿Conoce el personal la política de uso de los servicios de red?		
	Control de acceso al sistema operativo	¿Conoce el personal los procedimientos de inicio de sesión seguro?		
		¿Conoce el personal el uso de las utilidades del sistema?		
	Control de acceso a aplicaciones e información	¿Conoce el personal las restricciones de acceso a la información?		
		¿Es consciente el personal de la protección del aislamiento de sistemas sensibles?		
	Informática móvil y teletrabajo	¿Conoce el personal la política sobre el uso de la informática móvil y las comunicaciones?		

		¿Conoce el personal la política sobre el uso de tecnologías portuarias/ navales y los sistemas de teletrabajo?		
Adquisición, desarrollo y mantenimiento de sistemas de información	Controles criptográficos	¿Conoce el personal la política de uso de claves criptográficas y equipos relacionados?		
Gestión de incidentes de seguridad de la información	Notificación de incidentes y puntos débiles en materia de seguridad de la información	¿Conoce el personal los procedimientos de notificación de incidentes relacionados con la seguridad de la información?		
		¿Conoce el personal los procedimientos de notificación de fallos de seguridad?		
Gestión de la continuidad de las actividades	Gestión de la continuidad de las actividades	¿Conoce el personal el plan de continuidad de la actividad y el vínculo del plan de recuperación en caso de catástrofe par sus funciones?		

11.2 Anexo B: Cuestionario sobre prácticas de seguridad

El siguiente cuestionario puede distribuirse a los puertos para captar la madurez de sus prácticas de ciberseguridad. También puede distribuirse a las compañías marítimas y los armadores para que informen y evalúen las prácticas de seguridad aplicadas y seguidas:

Cuestionario para puertos y operadores marítimos sobre concienciación de seguridad

Información (opcional)

Empresa	xxxxxx
Nombre	xxxxx
Función	xxxxx
Número de empleados	xxxxx
Actividad empresarial	xxxx
Sitio web	xxxxx
Correo electrónico	xxxxxx

Fecha

Estimada parte interesada del sector marítimo,

El objetivo de este cuestionario es conocer el nivel de concienciación en materia de seguridad de la infraestructura marítima crítica (IC) en términos de amenazas y vulnerabilidad de todas las capas de la IC, es decir, (a) infraestructura física, (b) equipos de infraestructura de telecomunicaciones (c) software (d) servicios y aplicaciones (e) datos (f) usuarios (personas y cosas externas/internas). Además, se buscará una visión general de los servicios y los usuarios en relación con la vulnerabilidad.
El cuestionario pretende identificar si:

- Los operadores marítimos han establecido un plan de protección (plan de protección portuaria y política de protección de las TIC), en qué medida se aplica y qué objetivos tiene;
- Los empleados y usuarios marítimos son conscientes de los problemas de seguridad relacionados con sus actividades cotidianas;
- Se ofrece formación de concienciación sobre seguridad de la información, así como su eficacia;
- Existen interrelaciones entre las Autoridades Competentes y las IC marítimas (por ejemplo, los puertos) y por qué razones.

A efectos de esta encuesta, sólo se tienen en cuenta las IC marítimas en su calidad de operadores (es decir, los puertos que son simultáneamente arrendadores y operadores O explotadores de terminales). Aunque la encuesta se refiere a los puertos, es aplicable a cualquier IC marítima.

Las respuestas se considerarán confidenciales y sólo se comunicarán las cifras agregadas.

Para más información, puede ponerse en contacto con

xxxxxx

Plan de protección portuaria

1. ¿Ofrece el Puerto un plan de gestión de la seguridad bien definido?

- ☐ Sí - pase a la pregunta 1a
- ☐ No - pase a la pregunta 2

1a. ¿Qué modelo de gestión de la seguridad adopta? [Elija sólo una opción]

- ☐ Interno - por ejemplo, de un departamento específico o de una persona o personas del Puerto (por ejemplo, PFSO)
- ☐ Externo - por ejemplo, de otra empresa u organización o de expertos externos
- ☐ Otros

1b. ¿Cuál describe mejor su percepción de la seguridad: [Elija sólo una opción]?

- ☐ No afecta/influye en sus actividades empresariales
- ☐ No es su primera prioridad, pero piensa tenerla en cuenta en el futuro
- ☐ Comprende su necesidad, pero es demasiado caro para considerarla

1c. ¿Qué sistemas de seguridad cubre su plan de seguridad? [Elija los que considere oportunos].

- ☐ PBIP
- ☐ ISO 9001, ISO 14001 (Servicios de puertos de cruceros)
- ☐ ISO 27001
- ☐ ISO 27002
- ☐ ISO 28000
- ☐ Otros: PERS (Sistema de Revisión Ambiental Portuaria, para toda la zona portuaria)
- ☐ Otros (Cuáles:_____)

1d. ¿Su Esquema de Seguridad identifica y analiza en profundidad los siguientes aspectos?

		Nuestro Plan de Seguridad lo cubre, y...	
Actividades	Nuestro plan de seguridad no lo cubre.	los interesados presentan documentos válidos, pero no los analizamos.	mantenemos una base de datos activa sobre ellos y disponemos de procesos específicos detallados para los análisis
Planes de protección de buques	☐	☐	☐
Oficiales de protección de buques	☐	☐	☐

Actividades	Nuestro plan de seguridad no lo cubre.	Nuestro Plan de Seguridad lo cubre, y...	
		los interesados presentan documentos válidos, pero no los analizamos.	mantenemos una base de datos activa sobre ellos y disponemos de procesos específicos detallados para los análisis
Vigilantes de seguridad de la empresa	☐	☐	☐
Equipamiento de a bordo	☐	☐	☐
Planes de protección de las instalaciones portuarias correspondientes	☐	☐	☐
Oficiales de protección de instalaciones portuarias	☐	☐	☐
Determinados equipos de seguridad	☐	☐	☐
Determinados dispositivos de seguridad	☐	☐	☐
Control de las actividades de personas y mercancías	☐	☐	☐
Comunicaciones seguras	☐	☐	☐
Acceso seguro en los sectores portuarios (vigilancia, control)	☐	☐	☐
Política de ciberpuertos	☐	☐	☐
Otros (especifique)	☐	☐	☐
No sé	☐		

2. ¿Ha tenido en cuenta las cuestiones de seguridad en las siguientes actividades del Puerto en los últimos 12 meses? En caso afirmativo, ¿sus reacciones fueron proactivas o reactivas?

Actividades	No se tuvieron en cuenta las cuestiones de seguridad	Sí, se tuvieron en cuenta las cuestiones de seguridad	
		Naturaleza de la acción	
		proactiva	reactiva
Mejoras en sus servicios/productos/negocios/ cadenas de suministro	☐	☐	☐
Cumplimiento de la normativa	☐	☐	☐
Mejoras en el funcionamiento de sus sistemas informáticos	☐	☐	☐

Actividades	No se tuvieron en cuenta las cuestiones de seguridad	Sí, se tuvieron en cuenta las cuestiones de seguridad	
		Naturaleza de la acción	
		proactiva	reactiva
Mejoras en el funcionamiento de los sistemas de entrada/salida/perímetro de sus instalaciones portuarias	☐	☐	☐
Mejoras en el perfil de su empresa y en el nivel de confianza de sus usuarios y servicios	☐	☐	☐
Cumplimiento de la legislación de la UE que influye en sus operaciones y cadenas de suministro internacionales	☐	☐	☐
Privacidad y protección de datos	☐	☐	☐
Seguridad del personal y de los usuarios	☐	☐	☐
Acceso seguro en los sectores portuarios	☐	☐	☐
No sé	☐		

3. Seleccione tres (3) categorías principales de reglamentos/legislación que han influido/van a influir en su funcionamiento y medidas de seguridad en los últimos/próximos 12 meses. Indique si tiene en cuenta algún proyecto de seguridad en sus selecciones.

Tipos de reglamentos	En los últimos 12 meses	En los próximos 12 meses	Proyectos de seguridad en curso/en estudio
Auditoría interna:			
PBIP	☐	☐	☐
ISM	☐	☐	☐
Familias de normas ISO	☐	☐	☐
Familias OHSAS 18000	☐	☐	☐
Sarbanes-Oxley	☐	☐	☐
Reglamento (CE) nº 725/2004	☐	☐	☐
Normas SOLAS/MARPLE			
Directiva 2008/114/CE del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.	☐	☐	☐
Protección de datos (por ejemplo, GDPR, NIS, NISII, ISO 27000/27001/27002/27005, ISO15048, ISO18045)	☐	☐	☐

Tipos de reglamentos	En los últimos 12 meses	En los próximos 12 meses	Proyectos de seguridad en curso/en estudio
Normativa sectorial (por ejemplo, la norma de seguridad de datos PCI)	☐	☐	☐
Reglamento de aduanas y autoridades financieras	☐	☐	☐
Otros (Problemas con la aduana _____)	☐	☐	☐
Otros (Ningún problema con las autoridades financieras _____)	☐	☐	☐
Otros (especifique _____)	☐	☐	☐

4. Seleccione cinco (5) problemas de ciberseguridad en términos de importancia (1 = menor importancia, 5 = mayor importancia) para su empresa. ¿Tiene un plan para abordar estos problemas de seguridad?

Cuestiones de seguridad cibernética	Importante cuestión de seguridad	Plan de respuesta		
		Ahora	Próximos 12 meses	Ningún plan
Difusión segura de datos (a autoridades competentes, proveedores de la cadena de suministro, compañías marítimas, etc.)	☐	☐	☐	☐
Almacenamiento seguro de datos	☐	☐	☐	☐
Acceso (físico) a/desde las instalaciones portuarias	☐	☐	☐	☐
Servicios portuarios seguros (gestión de contenedores, GNL, servicios de la cadena de suministro)	☐	☐	☐	☐
Identificadores por radiofrecuencia (RFID)	☐	☐	☐	☐
Dispositivos móviles (por ejemplo, PDA, teléfonos inteligentes)	☐	☐	☐	☐
Sistemas automatizados de control de fronteras (ABC)	☐	☐	☐	☐
Almacenamiento móvil (por ejemplo, memorias USB, unidades portátiles)	☐	☐	☐	☐
Telefonía de voz sobre IP	☐	☐	☐	☐
Servicios web	☐	☐	☐	☐
Redes inalámbricas	☐	☐	☐	☐
Comunicación segura por satélite	☐	☐	☐	☐
Nuevos sistemas operativos	☐	☐	☐	☐

Cuestiones de seguridad cibernética	Importante cuestión de seguridad	Plan de respuesta		
		Ahora	Próximos 12 meses	Ningún plan
Criptografía del correo electrónico	☐	☐	☐	☐
Criptografía del disco duro	☐	☐	☐	☐

Prácticas de seguridad

5. ¿Cómo comprueba el nivel de seguridad de su empresa? [Elija más de una opción si es necesario].

- ☐ Auditoría interna (del Departamento de Seguridad)
- ☐ Auditoría externa
- ☐ Evaluación interna del personal
- ☐ Otros
- ☐ No disponemos de tales procedimientos

6. Seleccione cinco (5) actividades principales de seguridad en términos de importancia (1 = menor importancia, 5 = mayor importancia) para su Puerto. Seleccione de forma independiente cinco (5) actividades principales de seguridad en función del tiempo de ejecución necesario (1 = poco tiempo, 5 = mucho tiempo):

	Importancia	**Tiempo de ejecución**
Cumplimiento del ISP	☐	☐
Cumplimiento de las normas ISO27001, 27005	☐	☐
Gestión de la continuidad de las actividades	☐	☐
Gestión de riesgos y seguridad	☐	☐
Búsqueda, desarrollo e integración de sistemas informáticos	☐	☐
Gestión del control de acceso	☐	☐
Comunicaciones y gestión de operaciones	☐	☐
Seguridad física	☐	☐
Protección de los trabajadores (seguridad)	☐	☐
Actualizaciones de servicios y productos	☐	☐
Gestión de la seguridad	☐	☐

	Importancia	Tiempo de ejecución
Política de seguridad (cibernética)	☐	☐
Privacidad - Protección de datos	☐	☐
Rendición de cuentas	☐	☐
Plan de recuperación en caso de catástrofe	☐	☐

7. ¿Cómo aborda / resuelve los siguientes problemas de seguridad en su Puerto?

Cuestiones de seguridad:	Ninguna consideración	Buenas prácticas	Métodos propios
Incidentes de ciberseguridad - Ataques	☐	☐	☐
Continuidad de las actividades	☐	☐	☐
Resiliencia empresarial	☐	☐	☐
Gestión del ciberriesgo	☐	☐	☐
Gestión de riesgos físicos	☐	☐	☐
Privacidad y protección de datos	☐	☐	☐
Mecanismos de seguridad en la oferta de servicios portuarios	☐	☐	☐

8. Cuando colabora con otras empresas (por ejemplo, subcontratación, contratistas externos, terceros), ¿cuál de los siguientes aspectos considera necesario en materia de seguridad?

☐ Sus colaboradores tienen y siguen una política de seguridad auditable

☐ Sus colaboradores están obligados a utilizar/respetar su propia política de seguridad y sus preocupaciones en materia de seguridad

☐ Sus colaboradores cumplen la norma ISO 27001

☐ Ninguna de las opciones anteriores

☐ Otros

9. ¿Ha realizado alguna vez una evaluación de riesgos físicos?

☐ Sí

☐ No

10. ¿Con qué frecuencia informa sobre los riesgos e incidentes de seguridad física y a quién?

	Frecuencia				
	A diario	Mensual mente	Por trimestre	Por semestre	Nunca
Oficial de protección de instalaciones portuarias	☐	☐	☐	☐	☐
Empresa de seguridad (externa)	☐	☐	☐	☐	☐
Policía	☐	☐	☐	☐	☐
Aduanas	☐	☐	☐	☐	☐
Autoridades competentes (Cuáles:_____)	☐	☐	☐	☐	☐
Compañías de seguros	☐	☐	☐	☐	☐
Bancos e instituciones financieras	☐	☐	☐	☐	☐
Contratistas y partes interesadas	☐	☐	☐	☐	☐
Cámara de Comercio (u organización similar)	☐	☐	☐	☐	☐
Autoridad Nacional de Certificación	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐

11. ¿Ha realizado alguna vez una evaluación de riesgos cibernéticos?

☐ Sí
☐ No

12. ¿Con qué frecuencia informa sobre los riesgos e incidentes de ciberseguridad y a quién?

	Frecuencia				
	A diario	Mensual mente	Por trimestre	Por semestre	Nunca
Oficial de Ciberseguridad Portuaria	☐	☐	☐	☐	☐
Empresa de seguridad (externa)	☐	☐	☐	☐	☐
Autoridades públicas (por ejemplo, Policía	☐	☐	☐	☐	☐

	Frecuencia				
	A diario	Mensual mente	Por trimestre	Por semestre	Nunca
Compañía marítima	☐	☐	☐	☐	☐
Autoridades competentes (por ejemplo, CERT, CSIRTS, ISAC, Ministerio)	☐	☐	☐	☐	☐
Compañías de seguros	☐	☐	☐	☐	☐
Bancos e instituciones financieras	☐	☐	☐	☐	☐
Contratistas y partes interesadas	☐	☐	☐	☐	☐
OMI, AESM (u organización marítima similar)	☐	☐	☐	☐	☐
Autoridad Nacional de Certificación	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐
Otros (Cuáles _____)	☐	☐	☐	☐	☐

13. ¿Cómo se informa sobre cuestiones de seguridad? ¿Qué organización sería la más adecuada para recibir formación sobre seguridad? ¿Qué temas le interesan más? (Puede elegir varias opciones)

Organizaciones	Tecnologías de seguridad/ Implantación	Políticas de seguridad	Evaluación de riesgos	Privacidad-Protección de datos
Consultores de seguridad (empresas privadas)	☐	☐	☐	☐
Universidad	☐	☐	☐	☐
Organismo nacional	☐	☐	☐	☐
Internet	☐	☐	☐	☐
Órgano gubernamental	☐	☐	☐	☐
Cámaras de Comercio	☐	☐	☐	☐
Asociaciones industriales u organismos profesionales (por ejemplo, OMI, AESM, ENISA, NIST)	☐	☐	☐	☐
Prensa, publicaciones científicas	☐	☐	☐	☐

14. ¿Qué normas de seguridad conoce?

ISO 9001	☐
PBIP	☐
ISM	☐
Inspecciones SIRE / ATB	☐
ISA/IEC-62443	☐
Solicitud de inspección de US Barge and Inland ATB	☐
Inspección EBIS	☐
ISO/IEC 2700x	☐
ISO 20858	☐
ISO 15408, ISO18045	☐
Foro de Seguridad de la Información	☐
CobIT	☐
Biblioteca de Infraestructuras de Tecnologías de la Información (ITIL)	☐
Integración del Modelo de Madurez de las Capacidades (CMMI)	☐
SEISMED	☐
Ninguna de las opciones anteriores	☐
Otros (Cuáles _____)	☐
Otros (Cuáles _____)	☐
Añada más si es necesario	

15. ¿Cuál es la situación de su Puerto con respecto a las siguientes actividades de seguridad?

Actividad	En curso	En marcha en los próximos 12 meses	No previsto
Acceso físico mediante tarjetas inteligentes	☐	☐	☐
Acceso físico mediante tarjetas de identificación en papel	☐	☐	☐
Acceso físico mediante sistemas automatizados de control de fronteras (ABC)	☐	☐	☐

Actividad	En curso	En marcha en los próximos 12 meses	No previsto
Uso de diferentes tecnologías de autenticación para el acceso físico (por ejemplo, tarjetas de proximidad, tarjetas inteligentes, biometría).	☐	☐	☐
Utilización de sistemas de detección de intrusos	☐	☐	☐
Filtros antivirus y antispam actualizados	☐	☐	☐
Uso de cortafuegos	☐	☐	☐
Inspecciones (no planificadas) en buques	☐	☐	☐