European Commission

Programa de Monitorização de Rotas Marítimas Críticas, Apoio e Mecanismo de Avaliação (CRIMSON III)

Cibersegurança na Infraestrutura Marítima Crítica

Reflexão dos portos africanos

Service for Foreign Policy Instruments

COMISSÃO EUROPEIA
Serviço de Cooperação EuropeAid
Instrumento de Estabilidade/ Contrato n. N.º IFS/2019/410-525

Apresentado a:
Ondrej Vosatka
Serviço de Instrumentos de Política Externa (FPI)
FPI.1 - Paz e Estabilidade - Ameaças e Desafios Globais e Inter-regionais
EEAS 02/9A Rond Point Schuman, Bruxelas

Contrato n.º. No IFS/2019/410-525

Data: 20/04/2023

Autores:
Nineta Polemi, Professora de cibersegurança, dpolemi@gmail.com
Christophe Van Maele, Perito marítimo, cvanmaele@portconsult.eu

Este trabalho foi coordenado pela Evelyn Vancollie, coordenadora do projeto CRIMSON

Este estudo é financiado pelo Serviço do Instrumento de Política Externa (FPI) da União Europeia através do Mecanismo de Monitorização, Apoio e Avaliação das Rotas Marítimas Críticas (CRIMSON III), implementado pela RUSI Europe. Foi apoiado pela EU CyberNet.

Este relatório foi elaborado com o apoio da UE. O conteúdo deste relatório é da exclusiva responsabilidade dos seus autores e não pode, de forma alguma, ser considerado como reflectindo as opiniões da UE.

Table of Contents

Lista de acrónimos 5

Lista de figuras 7

Sumário executivo 8

1. Introdução 10

2. O ecosistema cibernético complexo 11

3. A União Europeia (UE) e os portos africanos 14

3.1. Introdução 14

3.1.1. Portos africanos 15

3.1.2. Negócio marítimo UE-África 17

4. Conceitos de segurança marítima 19

4.1. Introdução 19

4.2. Conceitos e terminologia de segurança 19

4.3. Cibertecnologia e física marítima 20

4.3.1. Digitalização marítima acelerada 22

4.4. Incidentes de segurança e atuadores de ameaças 22

4.4.1. Tipos de atacantes 22

4.4.2. Incidentes de segurança 23

4.4.2.1. Acidentes de segurança 25

4.4.2.2. Ciberataques 25

4.4.2.3. Ataques de TI/TO 28

4.4.2.4. A utilização de computadores para comunicar entre as partes interessadas permite uma ação eficiente e em tempo real quando necessário. Cadeia de abastecimento e ameaças híbridas 29

4.4.2.5. Vectores de ameaça 31

5. Normas e estratégias de proteção do transporte marítimo 33

5.1. Introdução 33

5.1.1. Estratégia Europeia de Segurança Marítima (EUMSS) 33

5.1.2. Normas de segurança marítima 34

5.1.2.1. O código ISPS 36

5.1.2.2. Outros códigos importantes 37

5.1.3. Normas de cibersegurança 38

5.1.3.1. ISO snormas para a proteção das ICI marítimas 38

5.1.3.2. Normas ISA, ANSI para ACS 39

5.1.3.3. Categorização das normas 40

5.2. Legislação de segurança 41

5.3. Legislação sobre cibersegurança 41

6. Boas práticas de Segurança Marítima 45

6.1. Introdução 45

6.2. Governação da segurança marítima 45

6.3. Higiene da cibersegurança dos operadores 46

6.4. Gestão da proteção marítima 47

6.4.1. Gestão da segurança (segurança física) 48

6.4.2. Gestão da cibersegurança 54

6.5 Ciber-resiliência marítima 57
6.6 Factores humanos 58

7. Práticas de segurança dos portos em África 60
7.1. Os portos do Golfo da Guiné 60
7.2. Organização da segurança portuária em África 60
7.3. Iniciativas internacionais para os portos africanos 62
7.4. Riscos cibernéticos em África 63

8. Conclusões 66

9. Recomendações 67
9.1. Recomendações para os portos da África Subsariana 67
9.2. Recomendações aos intervenientes marítimos africanos 68
9.3. Apoio à gestão de topo 68
9.4. Formação de sensibilização para a cibersegurança 69
9.5. Procedimentos, directrizes e instruções de cibersegurança 69
9.6. Serviços e funções críticos na organização 69
9.7. Avaliação dos riscos de cibersegurança 69
9.8. Plano de gestão da cibersegurança 69
9.9. Cibersegurança da cadeia de abastecimento 69
9.10. Gestão, resposta e recuperação de incidentes 69
9.11. Normas e quadros de cibersegurança 70
9.12. Recomendações gerais sobre a cibersegurança do porto 70
9.13. Recomendações para a UE: Rumo a uma colaboração estável entre a UE e África 72

10 Referências 74

11. Anexos: Questionários de segurança 77
11.1. Anexo A: Questionário de sensibilização para a governação da segurança 77
11.2. Anexo B: Questionário sobre práticas de segurança 81

Lista de acrónimos

AI	Inteligência artificial
AIS	Sistema de identificação automática
Sistema CCTV	Circuito fechado de televisão
CI	Infra-estruturas críticas
CII	Infra-estruturas críticas de informação
CISO	Responsável principal pela segurança da informação
COP	Código de conduta
COSCO	Companhia de navegação marítima da china
CSA	Avaliação de cibersegurança
CSI	Iniciativa para a segurança dos contentores
CSIRT	Equipa de resposta a incidentes de segurança informática
CSO	Responsável pela segurança da empresa
CSP	Plano de segurança cibernética
CYSO	Responsável pela cibersegurança
DA	Autoridades designadas
DDoS	Negação de serviço distribuida
DSP	Fornecedores de serviços digitais
ECDIS	Sistema de informação e visualização de correio eletrónico
EEAS	Serviço europeu para ação externa
EMSA	Agência europeia da segurança marítima
ENISA	Agência da união europeia para a cibersegurança
EUMSS	Estratégia europeia de segurança marítima
GDPR	Regulamento geral sobre proteção de dados
GMDSS	Sistema mundial de socorro e segurança marítima
GMN	Rede mundial MTCC
IACS	Associação internacional das sociedades de classificação
IAPH	Associação internacional de portos
Código IBC	Código internacional para a construção e o equipamento de navios que transportam produtos químicos perigosos a granel
ICS	Sistema de controlo industrial
ICT	Tecnologia da informação e da comunicação
ILO	Organização internacional do trabalho
Código IMDG	Código marítimo internacional para o transporte de mercadorias perigosas
IMO	Organização marítima internacional
Código IMSBC	Código marítimo internacional de cargas sólidas a granel
IoT	Internet das coisas
ISAC	Centro de análise e partilha de informações
ISM	Gestão internacional de segurança
ISMS	Sistema de gestão da segurança da informação
ISPS	Proteção internacional dos navios e das instalações portuárias
LNG	Gás natural liquefeito
MSC	Companhia de navegação mediterrânea
MTCC	Centro de cooperação tecnológica marítima
NIS	Redes e sistemas de informação

NLF	Novo quadro legislativo
OES	Operadores que prestam serviços essenciais
PCS	Sistema portuário comunitário
PFSO – PSO	Oficial de proteção do porto (instalação)
PSA – PFSA	Avaliação da segurança do porto (instalação)
PSC	Controlo do estado do porto
PSO - PFSO	Oficial de proteção do porto (instalação)
PSP – PFSP	Plano de segurança do porto (instalação)
RA	Avaliação dos riscos
RFID	Identificador de radiofrequência
RIB	Barco insuflável rígido
RM	Gestão dos riscos
RMF	Quadro de gestão dos riscos
SCADA	Controle de supervisão e aquisição de dados
SCSO	Responsável pela cibersegurança do navio
Nível de Segurança 1	Medidas de proteção 1 do isps, medidas mínimas adequadas
Nível de Segurança 2	Medidas de proteção do nivel 2 do isps, medidas de proteção adicionais, mantidas por um período de tempo devido ao risco acrescido de incidente de proteção.
Nível de segurança 3	Nível de segurança 3 do isps, medidas de segurança adicionais específicas, mantidas por um período limitado de tempo quando for provável ou iminente um incidente de segurança
SeMS	Sistema de gestão de segurança
SMS	Sistema de gestão da segurança
SOC	Centro de operações de segurança
SOLAS	Salvaguarda da vida humana no mar
SOP	Procedimentos operacionais normalizados
SSO	Oficial de proteção do navio
SSP	Plano de proteção do navio
STCW	Formação, certificação e serviço de quartos dos marítimos
TI	Tecnologia da informação
TO	Tecnologia operacional
TOS	Sistema operacional do terminal
YARIS	Rede regional de partilha de informação da arquitetura de Yaoundé

Lista de figuras

Figura 1: Ambiente marítimo 11

Figura 2: Portos africanos 16

Figura 3: A proteção inclui a segurança e a cibersegurança 19

Figura 4: Taxonomia de activos dos portos marítimos da ENISA 20

Figura 5: Tecnologias dos navios 21

Figura 6: Tecnologias portuárias 22

Figura 7: Taxonomia proposta pela ENISA para os ataques à cadeia de abastecimento 30

Figura 8: Taxonomia das normas de segurança marítima 41

Figura 9: Abordagem da BIMCO à gestão da segurança 48

Figura 10: Matriz de apetência pelo risco 55

Figura 11: Abordagem da BIMCO para a gestão da cibersegurança 56

Figura 12: Arquitetura SAURON de segurança física e cibernética 57

Figura 13: Resiliência marítima 57

Figura 14: Objectivos de segurança das IET 58

Figura 15: Região Marítima do Golfo da Guiné 60

Figura 16: Sistema de controlo do perímetro TO 62

Sumário executivo

Os portos comerciais modernos são uma infraestrutura crítica altamente dependente dos sistemas de informação. A segurança de um porto depende, portanto, da integridade dos activos físicos e cibernéticos. Apesar das provas de que os portos estão a tornar-se alvos de piratas informáticos, cujos ataques podem afetar tanto os activos cibernéticos como os físicos e interromper as operações, há demasiados portos com uma segurança cibernética inadequada. Ameaças físicas, incidentes e acidentes com os activos físicos (terminais, portões, edifícios) das infra-estruturas marítimas ou ciberameaças e ataques aos activos cibernéticos (sistemas comunitários portuários, sistemas de navegação) podem pôr em risco as operações marítimas, perturbar as cadeias de abastecimento e destruir o comércio internacional.

Esta investigação documental fornece uma avaliação dos conceitos de proteção marítima (segurança e cibersegurança) disponíveis para os portos, bem como das normas, metodologias, melhores práticas, ferramentas e quadros de gestão da segurança, e analisa os regimes jurídicos e regulamentares existentes. Além disso, o relatório apresenta as ciberameaças e os ataques que o ecossistema marítimo (portos, navios, empresas marítimas, autoridades, cadeias de abastecimento marítimo) enfrenta devido à rápida digitalização. As consequências e os impactos destas ameaças para o operador marítimo, as partes interessadas, as economias e a segurança nacional podem ser significativos. O presente documento apresenta normas, estratégias e instrumentos jurídicos e políticos em matéria de cibersegurança, a fim de servir de exemplo dos esforços envidados para enfrentar de forma holística os desafios da cibersegurança marítima. São apresentadas metodologias, ferramentas e directrizes de gestão do risco baseadas nas normas, a fim de sensibilizar os portos para as abordagens internacionais existentes. O cumprimento das normas e das estratégias de segurança existentes reforça a resiliência das operações, das cadeias de abastecimento e do comércio internacionais.

O relatório também capta o nível de sensibilização para a segurança dos portos da África Subsariana em comparação com os esforços europeus. Os dois questionários em anexo, elaborados pelos autores, podem ser distribuídos aos intervenientes marítimos africanos para autoavaliação do nível de governação da segurança (Anexo A) e do nível de maturidade da sua sensibilização e práticas (Anexo B). Os questionários podem igualmente ser utilizados para melhorar o seu nível de preparação em matéria de segurança. Por último, são feitas recomendações práticas à CE sobre a forma de estabelecer melhores relações com os portos africanos para aumentar as suas capacidades de segurança. O relatório serve para alertar os ministérios marítimos e os governos para as questões que devem ser consideradas.

As recomendações do relatório visam melhorar de forma holística a segurança nos portos africanos, incluindo recomendações específicas para a cibersegurança. A nível nacional, a legislação sobre cibersegurança deve ser revista e os quadros superiores dos portos devem ser incentivados a apoiar um investimento na governação da segurança, incluindo pessoal e recursos. Será necessária formação de sensibilização para a cibersegurança para todas as partes envolvidas e deverão ser constituídas equipas de cibersegurança. Recomenda-se a

realização de um inventário de todos os activos críticos, incluindo os ciberactivos, após o que uma avaliação dos riscos poderá identificar as ciberameaças, os riscos e as vulnerabilidades.

Com base nestes elementos, pode ser desenvolvido um plano de gestão da cibersegurança, incluindo a gestão, a resposta e a recuperação de ciberincidentes. Os fornecedores de equipamento de cibersegurança podem ter acesso remoto ao equipamento, pelo que a sua cibersegurança deve também ser avaliada. Existem normas e conhecimentos especializados em matéria de cibersegurança que podem ajudar os portos a criar e manter o seu escudo cibernético.

Há também recomendações para a UE sobre a forma de reforçar a colaboração UE-África nos domínios da segurança marítima, da cibersegurança e da segurança das cadeias de abastecimento. A UE deve procurar estabelecer colaborações estáveis entre os Ministérios dos Transportes Marítimos, as agências de segurança e os centros de análise e partilha de informações marítimas. A UE deve também procurar colmatar o défice de competências no domínio do ciberespaço com os seus parceiros africanos, nomeadamente através de exercícios realistas. O apoio além-fronteiras ao funcionamento de centros de operações de segurança marítima que prevejam e giram eficazmente os ciberataques e os incidentes de segurança reforçará também a colaboração. A harmonização dos esforços de certificação marítima também será útil, nomeadamente através de auditorias e avaliações conjuntas da segurança do equipamento marítimo para garantir a privacidade, a segurança, a transparência, a interoperabilidade, a responsabilização, a responsabilidade e o cumprimento da legislação e das directrizes internacionais em matéria de segurança. Por último, devem ser efectuadas análises comparativas regulares entre os portos da UE, os da região da África Subsariana e os de outras regiões do mundo. Tal seria útil para destacar as abordagens bem sucedidas da UE e da África em matéria de segurança e cibersegurança que podem ser reproduzidas noutras regiões.

1. Introdução

O sector marítimo sustenta as sociedades e as economias através do movimento de pessoas e bens vitais, como a energia (transporte de petróleo e gás) e os alimentos. A economia depende de forma crítica da proteção física e da segurança do movimento marítimo de carga e passageiros. No entanto, como a atividade marítima depende cada vez mais das tecnologias da informação e da comunicação (TIC) para otimizar as suas operações (por exemplo, da navegação à propulsão, da gestão da carga às comunicações de controlo do tráfego), a cibersegurança tornou-se um requisito essencial. Nos últimos anos, as ciberameaças tornaram-se uma ameaça crescente, alastrando a todo o ecossistema marítimo (dos portos às empresas marítimas e a outras infra-estruturas críticas interligadas, por exemplo, transportes e autoridades marítimas). A perturbação ou indisponibilidade das capacidades marítimas em matéria de TIC pode ter consequências potencialmente desastrosas, pelo que é cada vez mais necessário garantir a segurança física e a cibersegurança contra ataques físicos, cibernéticos e híbridos.

No presente relatório, a palavra "segurança" engloba a segurança física, a salvaguarda e a cibersegurança e deve ser tratada de forma holística e não fragmentada, uma vez que as infra-estruturas críticas marítimas incluem tanto os activos físicos como os cibernéticos.

A segurança física e a cibersegurança são desafios fundamentais a nível nacional e internacional. Os portos comerciais são infra-estruturas críticas (IC) e factores económicos fundamentais, pelo que a sua segurança é essencial no negócio marítimo e uma das maiores vantagens comerciais na era digital marítima internacional, competitiva e em rápido crescimento

Os portos são também nós indispensáveis das cadeias de abastecimento que envolvem muitas partes interessadas estratégicas, parceiros comerciais e actividades que interagem entre si. A segurança e a sustentabilidade são também preocupações importantes nas cadeias de abastecimento dos portos. Identificar e gerir as ameaças à cadeia de abastecimento e os seus efeitos e riscos em cascata são desafios importantes. As dificuldades devem-se, em parte, à complexidade induzida pelo grande número de actividades, processos, entidades e activos físicos e cibernéticos relacionados e interdependentes na cadeia de abastecimento. Metodologias e instrumentos de gestão de riscos específicos para gerir incidentes de segurança física e cibernética nos portos e nas suas cadeias de abastecimento são desafios importantes em matéria de segurança.

2. O ecosistema cibernético complexo

Os portos comerciais modernos, as companhias marítimas e os navios são altamente dependentes do funcionamento de sistemas TIC complexos e dinâmicos e de cadeias de abastecimento marítimo baseadas nas TIC e operam num ambiente marítimo complexo. O ambiente marítimo (Figura 1) envolve muitas partes interessadas e infra-estruturas que interagem entre si (autoridades, portos, companhias marítimas e de seguros, indústria naval, bancos, cadeias de abastecimento, outras infra-estruturas críticas), bem como activos (físicos e cibernéticos).

Figura 1 : Ambiente marítimo[1]

As infra-estruturas marítimas são consideradas críticas de acordo com as directivas NIS e NIS2 (directivas relativas à segurança das redes e dos sistemas de informação)[2], uma vez que a interrupção das suas operações e serviços teria um impacto negativo no comércio nacional, comunitário e internacional em geral, bem como, ocasionalmente, em vidas humanas.

nquanto infra-estruturas críticas, as infra-estruturas marítimas são obrigadas a manter a segurança (física e cibernética) de todos os seus activos das suas TIC, alojados e operados nas suas IC para prestar serviços portuários. As TIC marítimas podem ser vistas como um sistema físico cibernético com os seis níveis seguintes:

1. Camada de infra-estruturas (por exemplo, edifícios, plataformas, portões, marinas, centros de dados, terminais, navios)
2. Camada de telecomunicações (por exemplo, redes, equipamento de telecomunicações, satélites, estações de retransmissão, estações tributárias);

[1] (Polemi, 2017)

[2] (Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, 2016); (Negreiro, 2022)

3. Camada informática (por exemplo, sistemas de navegação/transmissão/ monitorização/comunidade portuária, SIG, sistemas de vigilância inteligentes, Internet das coisas (IoT));

4. Dados (por exemplo, dados marinhos e costeiros, dados comerciais);

5. Serviços Marítimos (e.g., faturação, navegação, gestão de bagagens/cargas/ navios/contentores, logística, serviços da cadeia de abastecimento);

6. Utilizadores: a. utilizadores internos (por exemplo, operadores, administradores, tripulação); b. utilizadores externos (por exemplo, autoridades portuárias, companhias marítimas, alfândegas, companhias de seguros, fornecedores de TI e da cadeia de abastecimento); e c. objectos inteligentes (por exemplo, contentores, navios, carga da tripulação, bagagem, veículos).

O primeiro (infraestrutura) e o sexto (utilizadores) são os níveis físicos das IC marítimas, enquanto os níveis 2 a 5 são os níveis cibernéticos. As partes interessadas do sector marítimo têm de garantir as dimensões de confidencialidade, integridade e autenticidade de todas as TIC, ou seja, a segurança dos bens físicos (segurança) e a segurança dos bens cibernéticos (cibersegurança).

As IC marítimas têm uma importância económica crescente e tornaram-se um alvo dos piratas informáticos, que lançam cada vez mais ataques físicos e cibernéticos aos sistemas de navegação global e aos sistemas de gestão da carga dos portos e dos navios. Estes ataques podem desativar um navio, desviar, desviar ou roubar carga, comprometendo também dados sensíveis de clientes ou empresas.

Do mesmo modo, os ataques aos Sistemas Operacionais de Terminais (TOS) dos portos, aos Sistemas Comunitários Portuários (PCS) (por exemplo, controlo de supervisão, SCADA, sistemas de controlo distribuídos e controladores lógicos programáveis) ou aos sistemas de navegação dos navios podem causar perturbações ou danos em dispositivos mecânicos críticos (por exemplo, gruas de contentores, sistemas mecânicos e de segurança que operam eclusas e barragens) e, pior ainda, podem causar a perda de vidas, roubar carga ou destruir um navio. Um ataque a um TOS de contentores pode também perturbar os serviços intermodais de contentores que envolvem o transporte marítimo, ferroviário e por camião.

Os TOS portuários mais antigos têm uma vida útil longa e funcionam frequentemente de forma independente, com políticas de senha e administração de segurança inadequadas, sem mecanismos e protocolos de proteção de dados, propensos a espionagem, interrupção e interceção, o que pode causar a perturbação de várias operações e serviços críticos dos portos e das cadeias de abastecimento. Os PCS são plataformas electrónicas complexas que ligam múltiplos sistemas operados por uma variedade de organizações do ecossistema marítimo e uma infinidade de fornecedores de TIC; a segurança dos PCS é tratada como uma "caixa negra" criptográfica, em que o funcionamento interno é oculto e só se conhecem os inputs e

os outputs[3]. As janelas únicas nacionais, que se baseiam no PCS, devem ser avaliadas e as políticas de segurança que as acompanham devem garantir a fiabilidade das suas operações.

Infelizmente, a maioria das partes interessadas do sector marítimo recorre a práticas de gestão da segurança não normalizadas e não harmonizadas, que se concentram nas ameaças e deficiências físicas, ignorando as cibernéticas. Os incidentes físicos e de cibersegurança podem pôr em causa o funcionamento dos portos, dos navios e de toda a cadeia de abastecimento, causando perturbações económicas, perturbações nos sistemas de transporte e no comércio internacional. Além disso, a perturbação das cadeias de abastecimento pode tornar-se um alvo para os terroristas internacionais se os portos e todas as entidades da cadeia não tiverem efectuado controlos de segurança adequados.

O presente relatório constitui um manual de sensibilização e um Guia de Boas Práticas que explica as principais questões relacionadas com a segurança (segurança e cibersegurança) da Infraestrutura de Informação Crítica (CII) marítima, as ciberameaças e os ataques que o ecossistema marítimo (portos, navios, empresas marítimas, cadeias de abastecimento marítimo) enfrenta devido à rápida digitalização. As consequências e os impactos destas ameaças para o operador marítimo, as partes interessadas, as economias e a segurança nacional podem ser imensos. São apresentadas normas, estratégias e instrumentos jurídicos e políticos em matéria de cibersegurança que servem de exemplos de esforços para enfrentar de forma holística os desafios da cibersegurança marítima. As metodologias, ferramentas e directrizes de gestão do risco baseadas nas normas são apresentadas para sensibilizar os portos africanos para as abordagens internacionais existentes. O cumprimento das normas e das estratégias de segurança existentes aumenta a resiliência e a colaboração, o que pode proteger as operações internacionais, as cadeias de abastecimento e o comércio. Por último, são apresentadas recomendações para os portos africanos e questionários para avaliar a maturidade dos portos em matéria de cibersegurança.

[3] (Acharya, 2019)

3. A União Europeia (UE) e os portos africanos

3.1. Introdução

Definições chave:

Instalação portuária: um local onde tem lugar a interface navio/porto; inclui zonas como os ancoradouros, os cais de espera e os acessos pelo lado do mar, consoante a instalação.**[Regulation (EC) No 725/2004]**.

Porto: uma área específica de terra e água, com limites definidos pelo Estado em que o porto se situa, contendo obras e equipamentos destinados a facilitar as operações de transporte marítimo comercial. [**Directive 2005/65/EC**].

As IC portuárias incluem as instalações portuárias (activos físicos dos portos), os activos cibernéticos e os utilizadores. De acordo com Alderton (1999), existem 3 tipos clássicos de propriedade e operação portuária, a saber Porto de Senhorio, Porto de Ferramentas e Porto de Serviços.

Responsabilidades da Autoridade Portuária (Fonte: Alderton, 1999)[4]			
Tipo de Porto	Infraestrutura	Superestructura	Estiva
Porto de Senhorio	Sim	Não	Não
Porto de ferramentas	Sim	Sim	Não
Porto de Serviços	Sim	Sim	Sim

O P*orto de Senhorio* é aquele em que o Estado, a autoridade portuária ou o conselho municipal são proprietários do terreno e arrendam o terminal a estivadores privados. O Estado fornece as infra-estruturas, como cais e terrenos para o terminal, enquanto o operador privado fornece a superestrutura e o equipamento, como gruas, armazéns, equipamento de terminal e outras instalações comerciais. Um exemplo é a Autoridade Portuária de Roterdão, que arrenda as infra-estruturas portuárias à European Combined Terminal (ECT).

O *porto de ferramentas* é a situação em que o Estado detém a infraestrutura e a superestrutura e a empresa privada de estiva fornece a mão de obra para a operação. A concorrência é muito elevada e os concursos são lançados para garantir os direitos. Exemplos disso são Houston nos Estados Unidos da América (EUA) e a maioria dos portos autónomos em França.

O porto de serviços é também conhecido como porto público ou abrangente. O Estado ou a autoridade portuária são proprietários da infraestrutura e da superestrutura e fornecem todos os serviços e instalações aos navios. Exemplos disso são a Autoridade Portuária de Singapura, que se tornou privada em 1997, e os portos da Índia, Israel, África do Sul e Gana.

[4] (Alderton, 1999)

A *camada física* dos portos inclui docas, cais, canais de acesso, entre outros. Em geral, as condições variam de terminal para terminal dentro de um porto. No entanto, todos os portos são desafiados a manter as suas infra-estruturas em ambientes marítimos adversos.

Superestrutura portuária: as disposições de superfície (por exemplo, para armazenamento), o equipamento fixo (por exemplo, armazéns e edifícios de terminais) e o equipamento móvel (por exemplo, gruas) localizados num porto para a prestação de serviços portuários relacionados com o transporte.

Estiva portuária: Inclui o carregamento e descarregamento e a estiva de carga, sob qualquer forma, a bordo dos navios nos portos.

Cada entidade com responsabilidades de autoridade portuária tem de identificar os seus activos críticos no domínio da sua responsabilidade e, consequentemente, avaliar o nível de risco.

Quase todos os activos estão ligados ao ciberespaço de três formas, nomeadamente 1) o sítio tecnológico e os sistemas de informação de comunicação (hardware/software); 2) os procedimentos operacionais da tecnologia e dos sistemas de informação de comunicação; e 3) as pessoas e os objetos inteligentes (por exemplo, IoT) que interagem com a tecnologia e os sistemas de informação de comunicação.

3.1.1. Portos africanos

As exportações africanas de bens e serviços registaram o seu crescimento mais rápido na última década, mas os volumes africanos continuam a ser baixos, representando apenas 3% do comércio mundial, de acordo com o Banco Mundial[5]. O papel limitado de África no comércio mundial reflecte-se nos contornos dos seus portos marítimos, que enfrentam desafios evolutivos em matéria de segurança, proteção e cibersegurança. No entanto, os portos marítimos são uma parte vital da cadeia de abastecimento em África, sendo o transporte marítimo a principal porta de entrada para o mercado global e tendo cada porto um interior de grande alcance que abrange frequentemente vários países sem litoral, que constituem um terço de África. Por conseguinte, o investimento e a modernização dos portos e das infra-estruturas de transporte conexas para fazer progredir a economia nacional e promover o desenvolvimento e o crescimento económico global de África são vitais.

Um estudo da PricewaterhouseCoopers (PWC) [6] mostra que os volumes económicos movimentados nos principais portos da África Subsariana se situam principalmente na África Ocidental e no Golfo da Guiné (ver figura abaixo).

[5] Uma participação maior e mais diversificada no comércio mundial é fundamental para alcançar a transformação económica de África, afirma o novo livro do Banco Mundial, 2022
[6] (Strengthening Africa's gateways to trade, 2018)

Figura 2: Portos africanos[7]

Os países do Golfo da Guiné dependem de mares protegidos e seguros para o seu desenvolvimento económico, comércio livre, transporte marítimo e preservação do ambiente marinho. Trata-se de uma grande região marítima que abrange 18 países com 500 milhões de habitantes e que se estende do Senegal a Angola, com mais de 5.700 km de costa. A região é uma importante rota de navegação internacional e representa 25% do tráfego marítimo africano. O petróleo e o peixe, entre muitos outros tipos de recursos naturais, são mercadorias importantes transportadas para outros países africanos e também para a Europa e outros países do mundo através de navios comerciais.

Os portos marítimos são a interface entre o mar alto e o interior. Constituem infra-estruturas marítimas de importância estratégica, através das quais todos os bens económicos têm de passar. Este facto torna-os altamente vulneráveis ao ataque de organizações criminosas e/ou grupos terroristas. Os ataques terroristas aos portos podem afetar gravemente as populações locais, as próprias infra-estruturas portuárias e as economias locais e regionais dependentes das actividades portuárias.

A UE continua a ser o principal parceiro comercial de África, embora a sua quota de comércio tenha diminuído, enquanto o comércio com a China aumentou. No continente africano, a África Ocidental é o maior parceiro comercial da UE na África Subsariana. A Europa importa da África Ocidental produtos acabados (peixe e têxteis), mas também produtos em bruto, como combustíveis e produtos agrícolas alimentares. Por outro lado, a África Ocidental importa da UE combustíveis refinados, produtos alimentares, maquinaria, produtos químicos e produtos farmacêuticos. Segundo a CNUCED, a África Ocidental é também o destino de investimento mais importante para a UE em África.[8]

Cabe a cada país decidir em que medida a sua legislação nacional em matéria de segurança e a Diretiva Internacional para a Segurança dos Navios e das Instalações Portuárias (ISPS) da

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

Organização Marítima Internacional (OMI) sejam aplicados e geridos de forma adequada. Existe a oportunidade de acompanhar os portos numa perspetiva alargada para aumentar a sua resiliência em termos de segurança. Este estudo servirá de manual com recomendações para melhorar a segurança dos portos na África Subsariana.

3.1.2. Negócio marítimo UE-África

A importância crítica do sector marítimo para os Estados-Membros europeus e as suas economias é claramente ilustrada pelo facto de existirem 329 portos comerciais europeus, pelos quais transitam 74% das mercadorias importadas e exportadas e 37% das trocas comerciais na União.

A UE e os EUA são os maiores parceiros comerciais da região de África[9]. O Pacote de Investimento Global Gateway África - Europa[10] visa apoiar África em:

- Acelerar a transição ecológica
- Acelerar a transição digital
- Acelerar o crescimento sustentável e a criação de emprego digno
- Reforçar os sistemas de saúde
- Melhorar a educação e a formação

O Centro Africano de Cooperação em Tecnologia Marítima (MTCC) foi lançado em Mombaça em 2017. Faz parte da Rede Global MTCC (GMN) financiada pela União Europeia[11]. O MTCC para África (MTCC África) está sediado na Universidade de Agricultura e Tecnologia Jomo Kenyatta (JKUAT), Campus CBD de Mombaça, em parceria com a Autoridade Marítima do Quénia (KMA) e a Autoridade Portuária do Quénia (KPA).

A MTCC África está centrada nos seguintes aspectos:

- Facilitar o cumprimento da Convenção Internacional para a Prevenção da Poluição por Navios (Anexo VI da MARPOL);
- Melhorar as capacidades na região, trabalhando com as administrações marítimas, as autoridades portuárias, os departamentos governamentais e as partes interessadas no sector do transporte marítimo, a fim de facilitar o cumprimento da regulamentação internacional em matéria de eficiência energética dos navios;
- Promover a adoção de tecnologias e operações com baixo teor de carbono no sector marítimo através de projectos-piloto;
- Sensibilizar para as políticas, estratégias e medidas de redução dos gases com efeito de estufa e outras emissões do sector do transporte marítimo;
- Demonstração de um sistema à escala-piloto de recolha de dados e comunicação de informações sobre o consumo de combustível dos navios, a fim de melhorar a compreensão dos armadores e das administrações marítimas a este respeito;
- Divulgar e partilhar os resultados e experiências do projeto através de acções de comunicação e visibilidade adequadas; e

[9] (Coulibaly, Kassa, & Zeufack, 2022)
[10] (UE-África: Pacote de investimento em portais globais,s.d.)
[11] (Centro para a Cooperação em Tecnológica Marítima lançado em Mombaça, 2017); (MTCC Africa, s.d.)

- Desenvolver e implementar estratégias para sustentar o impacto dos resultados e actividades do MTCC para além do período de duração do projeto.

Em 2021, o Eurostat declarou que o maior parceiro comercial de África é a Europa, exportando 33% dos seus bens para a Europa e importando 31% dos seus bens de lá. Isto equivale a importações de 142 mil milhões de euros e exportações de 146 mil milhões de euros de bens de/para África em 2021.

África depende fortemente de navios e portos para servir o seu comércio intercontinental, enquanto um terço dos países sem litoral recebe as suas mercadorias através de países com acesso ao mar. Isto significa que o transporte marítimo continua a ser a principal porta de entrada para a Europa.

O comércio marítimo de África é definido pela concentração do comércio internacional do continente nos portos marítimos. A CNUCED refere que os portos africanos representam apenas quatro por cento do volume global do comércio em contentores, grande parte do qual é constituído por importações de produtos manufacturados. Os portos africanos não correspondem às tendências mundiais em termos de rácios de contentorização e poderiam melhorar os seus volumes de tráfego portuário contentorizado e aumentar as mercadorias exportadas por contentor. Se mais carga fosse transportada por estrada do interior para os portos, mais navios porta-contentores entrariam nos portos, atraindo um maior tráfego internacional.

Para que tal aconteça, os portos e as redes de transporte do interior de África têm de modernizar as suas infra-estruturas e serviços portuários, melhorar o desempenho, aumentar os níveis de produtividade, mas também aumentar a sua segurança, a segurança portuária ISPS e as iniciativas de cibersegurança.

4. Conceitos de Segurança Marítima

4.1. Introdução

No nosso mundo preocupado com a segurança, é difícil recordar uma época em que a segurança não fosse uma prioridade. Hoje em dia, as acções no domínio da proteção do transporte marítimo melhoram todos os anos em várias regiões do mundo, o que resulta numa diminuição gradual dos acidentes, ferimentos e ataques físicos e cibernéticos. Mas este tipo de proteção nem sempre foi uma prioridade para os armadores e os portos marítimos. A mudança da reparação para a prevenção foi impulsionada por acidentes e ciberataques ocorridos no passado a bordo de navios, em portos marítimos e empresas marítimas. O fio condutor destes incidentes foi o facto de as regras existentes em matéria de segurança (segurança e cibersegurança) não terem sido seguidas à risca e não terem sido devidamente aplicadas na prática.

4.2. Conceitos e Terminologia de Segurança

A literatura internacional utiliza indistintamente os termos "segurança", "proteção", "cibersegurança", "segurança física" e "resiliência".

No presente relatório, como já foi referido, as IC marítimas são consideradas sistemas físico-cibernéticos com camadas físicas e cibernéticas. As partes interessadas do sector marítimo têm de garantir a segurança dos bens físicos (segurança) e a segurança dos bens cibernéticos dentro das camadas (cibersegurança). O objetivo da segurança marítima é proteger os bens físicos (por exemplo, navios, edifícios, marinas, centros de dados, carga) e as pessoas (por exemplo, pessoal, operadores, tripulação) contra vários tipos de ameaças físicas, por exemplo, incidentes intencionais e não intencionais, perigos e danos, como catástrofes físicas, tempestades no mar, incêndios, terrorismo, distúrbios sociais, contrabando de armas e drogas, pirataria. O objetivo da cibersegurança marítima é garantir a confidencialidade, a integridade e a disponibilidade de todos os activos cibernéticos (por exemplo, telecomunicações, TIC, dados, serviços) contra ciberameaças (por exemplo, phishing, spoofing, engenharia social (actividades maliciosas que utilizam interacções humanas), identidades mascaradas, acesso não autorizado, ataques distribuídos de negação de serviço (DDoS)).

A segurança inclui tanto a segurança como a cibersegurança conforme ilustrado na figura 3.

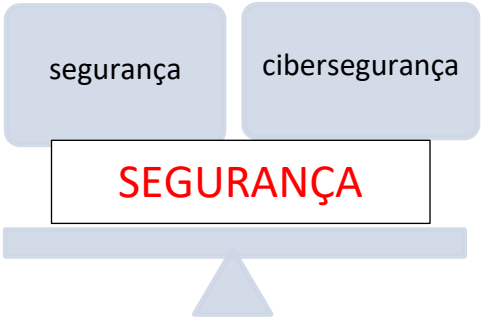


Figura 3 : A segurança inclui a segurança e a cibersegurança

Os activos físicos e cibernéticos podem ser expostos a ameaças se não tiverem sido implementados controlos/medidas e acções de atenuação adequados, deixando os activos vulneráveis a ameaças e à exploração. No caso de ocorrer um incidente de segurança infeliz, são activados os procedimentos de segurança de emergência, a recuperação de desastres e os planos de continuidade das actividades, sendo tomadas medidas para atenuar os riscos. Sempre que ocorre um incidente, é accionada uma série de medidas a nível nacional, em conformidade com os planos de emergência a bordo do navio (Planos de Segurança dos Navios), no porto marítimo (Plano de Segurança Portuária) e nas instalações portuárias (Planos de Segurança das Instalações Portuárias).

O fio condutor entre a segurança e a cibersegurança é o escudo de proteção aplicável em cada domínio. A construção deste nível de proteção é feita através de uma governação eficiente, tentando eliminar os riscos físicos e cibernéticos, evitar incidentes de segurança portuária e prevenir acidentes humanos. Um tem impacto no outro, por exemplo, se um ataque de cibersegurança numa instalação portuária de carga geral interromper subitamente a operação de manuseamento da grua, isso pode fazer com que a carga caia no porão do navio e causar ferimentos fatais aos trabalhadores portuários que se encontram em baixo. Por conseguinte, o presente estudo aborda **a segurança como a composição da segurança e da cibersegurança** e apresenta o modo como a regulamentação, as normas e as melhores práticas podem ser combinadas para dar resposta a ambas as componentes da segurança.

4.3. Cibertecnologia e física marítima

Os portos e os navios acolhem ICI complexas com activos físicos e cibernéticos utilizados para realizar as suas operações e prestar os seus serviços marítimos.

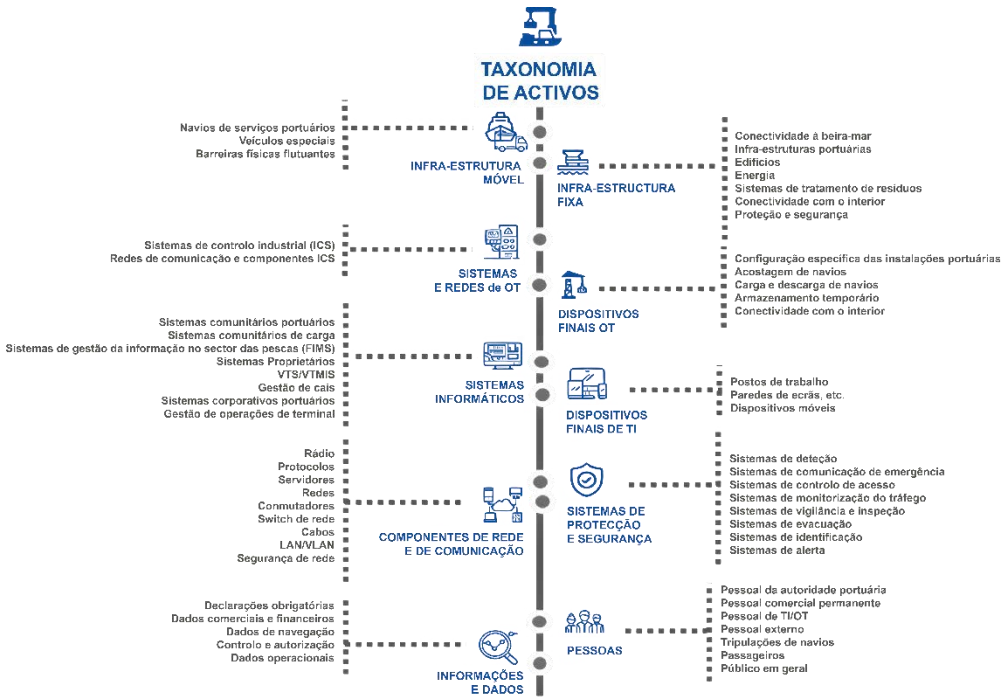


Figura 4: ENISA Taxonomia dos activos dos portos marítimos[12]

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

Os navios estão equipados com várias tecnologias, incluindo: Sistemas de posicionamento, Sistema de Informação e Visualização de Cartas Electrónicas (ECDIS), Sistemas de controlo e monitorização de motores, Sistema Global de Socorro e Segurança Marítima (GMDSS), Sistema de Identificação Automática (AIS), ICS SCADA marítimo. A figura seguinte ilustra as tecnologias a bordo:

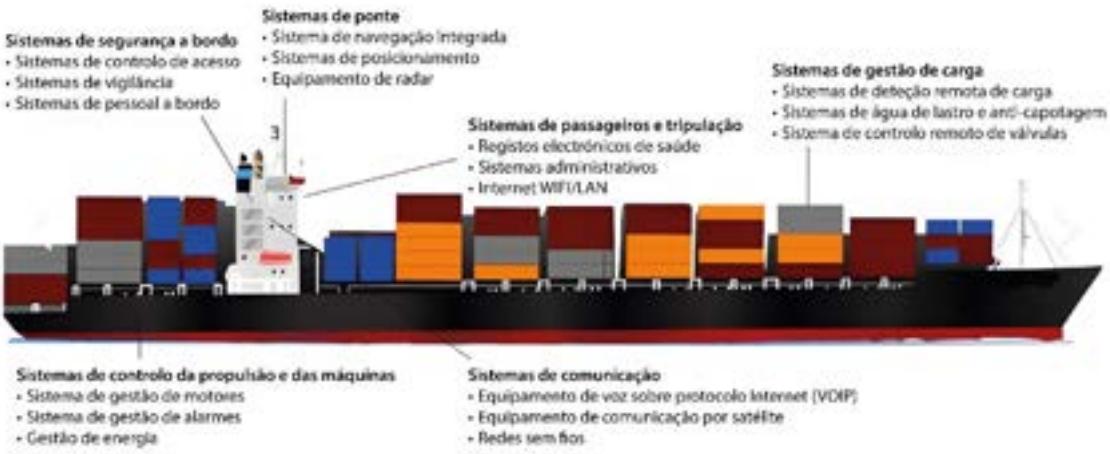


Figura 5 : Tecnologias de navios[13]

As tecnologias portuárias e dos navios são utilizadas para prestar serviços portuários e de cadeia de abastecimento marítimo, por exemplo:

- Serviços de atracação de navios
- Serviços de carga e descarga de navios
- Serviços de armazenamento temporário e de permanência
- Serviços de distribuição e transferência
- Serviços de apoio
- Serviços das autoridades
- Serviços de segurança
- Transporte de mercadorias (por exemplo, gás natural liquefeito (GNL), veículos, cereais)
- Serviços de cruzeiros e transporte de pessoas
- Serviços de gestão de contentores
- Serviços de transporte marítimo costeiro

[13] Fonte: https://www.hvassallo.com/practice-areas/maritime-cyber-security/; acedido em 17 de dezembro de 2022

Figura 6: Technologias de portos[14]

4.3.1. Digitalização marítima acelerada

A adoção de tecnologias emergentes, incluindo a inteligência artificial (IA), a 5G, os megadados, a IdC, a robótica e as tecnologias de satélite, está a ser utilizada para novos avanços marítimos, por exemplo, navios autónomos, inspeção rápida de portos, incluindo instalações de energia eólica, estações bentónicas submarinas, automatização de operações de prospeção sísmica geofísica e geotécnica, monitorização e gestão de navios.

A adoção acelerada das tecnologias digitais no ecossistema marítimo conduzirá a numerosas inovações em várias funções marítimas, por exemplo, o intercâmbio de quantidades maciças de informação utilizando redes avançadas de comunicações acústicas e ópticas, a automatização de decisões colectivas, a partilha de recursos complementares, a automatização da manutenção e das operações de portos e navios. No entanto, estas inovações futuras serão acompanhadas de novas ameaças físicas e cibernéticas. A governação da segurança (segurança e cibersegurança) será necessária para garantir que as autoridades portuárias, os armadores e todas as partes interessadas do sector marítimo disponham das ferramentas, dos conhecimentos e da estrutura necessários para maximizar o desempenho das suas infra-estruturas (portos, a bordo dos navios) em termos de segurança e atingir os seus objectivos de segurança, em conformidade com a legislação de segurança marítima e as melhores práticas internacionais.

4.4. Incidentes de segurança e atuadores de ameaças

Cada porto precisa de desenvolver uma governação de trabalho personalizada com práticas eficientes de gestão dos riscos (físicos e cibernéticos) que garantam a segurança das IC, das operações e dos serviços marítimos.

4.4.1. Tipos de atacantes

Os *cibercriminosos* são adversários que realizam uma ação ilegal utilizando meios digitais. Por exemplo, se o impacto do ataque for ilegal (p. ex., roubo, crime, vandalismo, terrorismo), o adversário é caracterizado como cibercriminoso. Os adversários são ainda classificados de acordo com as suas motivações, oportunidades e capacidades:

[14] Fonte: (Burt, 2021)

- *Actores intencionais:* os atacantes internos são uma classe de ameaças com conhecimentos pormenorizados de uma organização e dos seus sistemas.
- *Ciberterroristas:* realizam actividades violentas para influenciar a opinião pública e a tomada de decisões.
- *Hacktivistas / Activistas civis:* por razões ideológicas, realizam ataques para chamar a atenção para uma agenda política, social, religiosa ou moral.
- *Cibercriminosos (organizados):* o seu objetivo é obter lucros financeiros, influenciar eleições, abusar de pessoas. Todas as actividades criminosas tradicionais que são conduzidas através de meios digitais pertencem a esta categoria.
- *Script Kiddies:* agentes não maduros com poucos conhecimentos e capacidades, com o objetivo habitual de se divertirem, ganharem uma aposta ou um prémio.
- Os *atacantes patrocinados pelo Estado / espiões do governo* operam para obter acesso a informações privilegiadas, como propriedade intelectual, planos de negócios, roteiros, dados sobre o pessoal ou sobre os clientes, etc., e para conhecer as operações comerciais e a futura tomada de decisões.
- *Concorrentes / Agentes de espionagem industrial comercial* tentam obter uma vantagem comercial através do roubo de propriedade intelectual, documentação sobre operações e decisões comerciais ou dados de clientes.
- *Ciberguerreiros governamentais / Cibercaças individuais* são tipos de actores com motivações patrióticas. São diretamente controlados por uma nação ou são indivíduos ou grupos de pessoas movidos pelos seus valores políticos, sociais, étnicos ou religiosos.
- Os *cibervândalos / ciberpunks* têm como principal motivação a destruição de bens, motivados pela procura de satisfação pessoal e de domínio.
- *Os Blackhat Hackers / Crackers* tentam obter acesso a sistemas por curiosidade e ganho pessoal, que pode ir desde recompensas financeiras pela exploração de dados, produtos e sistemas obtidos, ou em termos de reputação e reconhecimento entre os seus pares.

Há também os *Actores Não Intencionais*, que são normalmente empregados sem formação ou imprudentes que ainda têm o potencial de causar danos à organização. Não têm intenções maliciosas, mas são mencionados porque as suas acções podem ainda representar um risco para a segurança.

4.4.2. Incidentes de Segurança

As operações portuárias e dos navios dependem cada vez mais da eficácia dos sistemas baseados em software para as operações, e os navios e portos que souberem tirar partido das novas tecnologias e soluções digitais estarão em melhor situação do que os outros. Por exemplo, a comunicação entre os navios e as operações portuárias de movimentação de carga exige a transferência de informações através de computadores. Estes sistemas de tecnologia da informação (TI) tratam de todas as tarefas administrativas de preparação, execução e manuseamento da carga. As máquinas de movimentação nos terminais, como as gruas de contentores, e as máquinas a bordo dos navios têm ligações digitais a outros sistemas de controlo remoto. Estas máquinas mecânicas com equipamento digital são designadas por sistemas de tecnologia operacional (TO). De um modo geral, pode dizer-se

que os sistemas de TO controlam o mundo físico, como as máquinas, enquanto os sistemas TI gerem os dados/informação. Estes últimos gerem o fluxo de informação digital (dados), enquanto os primeiros gerem o funcionamento dos processos físicos e as máquinas utilizadas para os executar. No mundo marítimo, a TO refere-se ao hardware, sistemas e software dos navios e dos portos que operam os navios e o equipamento de movimentação portuária e monitorizam e controlam os dispositivos e processos físicos, e a TI refere-se aos computadores e servidores dos escritórios utilizados para gerir o processamento da informação, incluindo software, hardware e tecnologias de comunicação.

Estes sistemas informáticos e de TO nem sempre estão bem protegidos contra um ciberataque. Os riscos dos sistemas de TI afectam principalmente as finanças e a reputação, enquanto os sistemas de TO podem afetar e ameaçar as infra-estruturas portuárias e até custar vidas. Os portos marítimos e os navios podem parecer alvos invulgares de ciberataques, mas estes ataques visam cada vez mais os operadores marítimos e são regularmente comunicados ataques bem sucedidos em todo o mundo. Por conseguinte, a cibersegurança está a tornar-se cada vez mais importante para resistir aos ciberataques no sector marítimo.

Durante muito tempo, os quadros superiores das empresas portuárias e marítimas consideraram a cibersegurança e a gestão dos riscos como uma tarefa do departamento de TI, mas esta situação está a mudar rapidamente, uma vez que todo o pessoal está envolvido na gestão e ajuda a atenuar os riscos cibernéticos.

O impacto de um ciberataque pode propagar-se aos bens físicos, por exemplo, um ciberataque pode desativar o sistema inteligente de deteção de incêndios e os sistemas automáticos de extinção de um navio-tanque de GNL num grande porto em África e provocar um incêndio. Os ciberataques e qualquer tipo de incidente de proteção/segurança podem ter um impacto negativo nas cadeias de abastecimento marítimo e no comércio local e internacional. Por exemplo, um ciberataque ao sistema eletrónico de navegação pode desorientar um navio, levando-o a colidir e a afundar-se à entrada de um grande porto da UE ou de África. Poderão ser necessárias semanas para remover os destroços e repor o porto em funcionamento, com prejuízos económicos, jurídicos e comerciais para as cadeias de abastecimento africanas e europeias causados pela interrupção do comércio.

Os navios podem ser utilizados como meio de transporte para terroristas ou para contrabandear armas para um país, mas também podem ser utilizados para detonar uma bomba no navio e fazer explodir uma parte crítica do porto. No entanto, um inquérito de 2018 sobre cibersegurança[15] revelou que poucas empresas de transporte marítimo estão preparadas para resistir a um ciberataque sem grandes danos. A necessidade de directrizes e de legislação relevante é mais do que evidente no sector. Os portos precisam de implementar um plano de governação eficaz que abranja procedimentos e processos de governação físicos e de cibersegurança.

[15] (Jørgensen, 2018)

4.4.2.1. Acidentes de segurança

Vários acidentes marítimos e desastres fatais de navios são considerados incidentes de segurança. Por exemplo, o naufrágio do RMS Titanic, em abril de 1912, foi um dos primeiros navios de passageiros a afundar-se, com a perda de mais de 1 500 vidas. Esta catástrofe e o elevado número de vítimas devem-se a uma navegação imprudente perto de icebergues e à insuficiência de botes salva-vidas para salvar todas as pessoas a bordo[16]. Outro exemplo é o naufrágio do Ferry M/S Estonia em 1994, em que a proa do convés de carga não estava fechada de forma estanque e se abriu durante uma tempestade, provocando o afundamento e a perda de mais de 850 passageiros[17]. Um acidente semelhante ocorreu com o Ferry Herald of Free Enterprise em 1987, provocando a perda de 197 pessoas e de todo o navio com a sua carga[18]. A explosão fatal do navio-tanque M/V Bow Mariner, em 2004, carregado com etanol, explodiu, afundou e deixou 21 tripulantes numa sepultura no mar. A razão para este desastre [19] foi a violação de várias normas de segurança que causaram a explosão e aumentaram o número de mortos. Um acidente mais recente, o desastre do Costa Concordia em 2012, foi causado quando o capitão navegou demasiado perto das rochas, resultando na perda do navio e de 32 vidas[20].

Nos portos marítimos, podem ocorrer muitos acidentes relacionados com as operações de descarga e carga dos navios, mas também nos terminais e na zona portuária comum. Um estudo realizado por R. Darbra e J. Casal[21] sobre centenas de acidentes ocorridos em portos marítimos concluiu que os acidentes mais frequentes foram as libertações de gás (51%), seguidas de incêndios (29%) e explosões (17%). Mais de metade dos acidentes ocorreram durante as operações de carga e descarga, mas os acidentes em armazéns de armazenagem, os acidentes em fábricas de produtos químicos e as operações na zona portuária também contribuíram significativamente para o número total. Um dos exemplos mais recentes de um acidente grave ocorreu no porto de Beirute em agosto de 2020, quando uma enorme explosão devastou partes de Beirute e foi atribuída à detonação de 2750 toneladas de nitrato de amónio que tinham sido armazenadas no porto de Beirute após a apreensão de um navio[22].

4.4.2.2. Ciberataques

Os ciberataques às infra-estruturas marítimas podem ser variados. Apresentam-se a seguir alguns exemplos de ciberataques recentes, a fim de chamar a atenção dos leitores para as potenciais ameaças de tais actos maliciosos e de aprofundar a análise dos mecanismos desses ataques.

- Em 10 de abril de 2020, um ataque de malware visou a Mediterranean Shipping Company (MSC)[23]. Por razões de segurança, os servidores da MSC foram desligados

[16] (Titanic, s.d.)
[17] (Langewiesche, 2004)
[18] (Desastre de ferry Herald of Free Enterprise – 1987, s.d.)
[19] (Shapira, 2006)
[20] (Costa Concordia: What happened, 2015)
[21] (Darbra & Casal, 2004)
[22] (A explosão do porto de Beirute, s.d.)
[23] (Hand, 2020)

para proteger os dados da empresa e o sítio Web da MSC foi retirado do ar. O ataque perturbou os processos de dados internos.

- Em 8 de julho de 2019, um ataque de malware visou um navio com destino ao porto de Nova Iorque, resultando na perda de dados críticos. A Guarda Costeira informou que a falta de estratégias de segurança no navio foi a principal razão para esse ataque[24]. Todos os membros da tripulação do navio partilhavam o mesmo login e password para o computador do navio. Além disso, o hacker aproveitou a utilização de dispositivos externos e a falta de software antivírus.
- Em março de 2019, um ataque de ransomware paralisou completamente a rede global da empresa de navegação Norsk Hydro quando esta foi vítima do ransomware LockerGoga. A Norsk Hydro estimou que os piratas informáticos tinham estado na sua rede durante duas a três semanas antes de serem descobertos. Mais de 22.000 computadores e milhares de servidores em cinco países foram afectados, e o LockerGoga encerrou a produção e as operações de escritório durante dias. Os danos foram estimados em 71 milhões de dólares[25].
- Em 2018, o governo chinês é suspeito de ter levado a cabo um ataque de ransomware a um contratante da Marinha dos EUA e de ter roubado dados de segurança altamente sensíveis, incluindo planos para um projeto de míssil supersónico[26].
- Em setembro de 2018, ciberataques atingiram os portos de Barcelona (Espanha) e San Diego (EUA). O ataque de ransomware ao porto de San Diego revelou-se uma infeção do malware SamSam[27]. O impacto limitou-se a algumas funções administrativas da autoridade portuária e não interrompeu as operações portuárias ou os movimentos dos navios. O porto de Barcelona não divulgou imediatamente o tipo de incidente, mas indicou que o ataque tinha perturbado os seus sistemas informáticos internos, embora não tenha afetado as operações dos navios ou do porto.
- Em julho de 2018, a China Ocean Shipping Company (COSCO) também foi vítima do ransomware SamSam. Quando o SamSam atacou, perturbou as redes da COSCO nos Estados Unidos, no Canadá, no Panamá, na Argentina, no Brasil, no Peru, no Chile e no Uruguai. Foram necessários 5 dias para que a empresa voltasse a estar online.
- O Grupo A.P. Moller-Maersk foi atingido por um ataque devastador em junho de 2017 devido ao malware NotPetya[28]. A Maersk teve de interromper as operações durante 10 dias para recuperar do ataque, o que implicou a reinstalação de 4000 servidores, 45 000 PC e 2500 aplicações. A Maersk terá perdido cerca de 300 milhões de dólares em receitas.

O quadro seguinte enumera as principais ciberameaças para 2022, de acordo com a Agência da União Europeia para a Cibersegurança (ENISA) e a Gestão do Risco Cibernético dos Portos.

[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)

Ciber ameaça	Ciber incidente			Referência
	Organização afetada	Data	Impacto	
Malware/ Ransomware	Sistemas TI	2022	Grande terminal petrolífero Europeu	https://www.france24.com/en/live-news/20220203-european-oil-port-terminals-hit-by-cyberattack
Malware/ Ransomware	Empresas petrolíferas	2022	Porto de Antuérpia	https://www.dw.com/en/belgium-investigates-cyberattack-on-energy-companies/a-60651892
Malware	Sistemas TI	2021	Tanque de petróleo Alemanha GmbH & Co. KG	https://www.bbc.com/news/technology-60215252
Malware/ Ransomware (Mailto)	Grupo Toll	2020	Destruição de dados	https://www.itnews.com.au/news/toll-group-hit-by-new-variant-of-mailto-ransomware-537537
Malware	Companhia de Navegação Mediterrânica (MSC)	2020	Falha de rede	https://www.wsj.com/articles/mediterranean-shipping-co-hit-by-network-outage-considering-potential-cyberattack-11586523861
Malware	CMA CGM	2020	Violação da segurança	https://www.reuters.com/article/uk-cma-cgm-cyber-idUKKBN26L2N0
Malware/ Ransomware	Serviços administrativos do porto	2018	Porto de San Diego e Barcelona	https://www.acronis.com/en-us/blog/posts/ransomware-attacks-sail-san-diego-and-barcelona/
Malware/ Ransomware	COSCO	2018	Avaria na rede 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	Destruição de dados	https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html
Violação de dados	O serviço do porto que controla o movimento e a localização dos contentores	2013	Porto de Antuérpia	https://www.bbc.com/news/world-europe-24539417

As mudanças geopolíticas também afectam a segurança das operações marítimas. Durante a guerra da Ucrânia em 2022, os navios que navegavam no Mar Negro e no Mar de Azov sofreram uma série de ciberataques. A Administração Marítima dos EUA (MARAD) informou que os navios foram vítimas de interferências no GPS, de falsificação do AIS e de interferências

nas comunicações. O Centro de Navegação da NATO e a Administração Marítima dos EUA comunicaram ataques DDoS a estes navios.

4.4.2.3. Ataques de TI/TO

Muitos navios ainda utilizam sistemas e tecnologias de informação de TI e TO que não foram concebidos para resistir a ciberataques. Se não estiverem devidamente protegidos, os piratas informáticos podem explorar as vulnerabilidades. Se conseguirem controlar remotamente o sistema do navio, podem apoderar-se dos sistemas de informação de comunicação de comando e controlo. Um navio é um sistema integrado de sistemas. É por isso que os sistemas das infra-estruturas de informação críticas do navio têm de ser definidos e avaliados, e a sua segurança tem de ser continuamente monitorizada e inspeccionada regularmente. Outras actividades que os hackers podem realizar são:

- falsificar os sistemas de navegação
- controlar o piloto automático do navio
- interferir com os radares do navio
- controlar os motores e a velocidade do navio
- desestabilizar os navios através da transferência/inundação de água de lastro
- danificar gravemente o equipamento, por exemplo, desligando um sistema de arrefecimento vital
- desligar sistemas vitais de carga, como a alimentação eléctrica dos frigoríficos
- desligar os sistemas de deteção e extinção de incêndios
- assumir o controlo do leme durante tempo suficiente para conduzir o navio para a doca a toda a velocidade

Por conseguinte, os navios devem utilizar soluções tecnológicas e princípios operacionais para evitar este tipo de situações. As soluções são descritas no presente estudo nos capítulos 5 e 6.

O mesmo se aplica aos portos, onde os sistemas informáticos e TO estão também em constante utilização. No domínio da segurança dos portos e dos terminais conformes com o ISPS, é importante ter em conta o seguinte:

- O Sistema de Gestão da Segurança (SGS) só é eficaz se for digitalizado.
- O sistema de cartões de identificação é eficaz se for um sistema digital baseado numa base de dados comum à qual as autoridades policiais e aduaneiras também têm acesso.
- o sistema de barreiras automáticas admite apenas pessoas com direito a entrar na zona.
- um sistema de monitorização do perímetro com um circuito fechado de televisão (CCTV) de alto desempenho ou outro sistema de câmaras tomará medidas inteligentes e poderá seguir as imagens de vídeo durante longos períodos de tempo.

Mais pormenores sobre este assunto estão incluídos abaixo.

4.4.2.4. A utilização de computadores para comunicar entre as partes interessadas permite uma ação eficiente e em tempo real quando necessário. Cadeia de abastecimento e ameaças híbridas

As cadeias de abastecimento marítimo são as veias sanguíneas do comércio e da economia mundiais e envolvem a colaboração transfronteiriça para oferecer serviços críticos complexos (por exemplo, gestão de contentores, transporte de veículos, armazenamento e transporte de GNL, cruzeiros). A maioria dos processos físicos num serviço marítimo (por exemplo, veículos e carga/descarga, distribuição e armazenamento de GNL) é executada com sistemas físicos mecânicos autónomos ou semi-autónomos e maquinaria (por exemplo, navios, camiões, gruas, portões/vedações electrónicas) sob o controlo de sofisticados sistemas de software logístico (por exemplo, sistemas ciber-físicos industriais, SCADA, sistemas de vigilância). Além disso, os navios de carga estão ligados aos portos e aos outros operadores através de uma infinidade de ligações de comunicação e de dados (por exemplo, comunicações por satélite ou radiocomunicações convencionais) e a sua navegação depende hoje em dia largamente de soluções electrónicas (por exemplo, navegação por satélite com GPS, Galileo ou Electronic Chart Display Information Systems, (ECDIS)). Assim, as cadeias de abastecimento marítimo podem ser vistas como sistemas físico-cibernéticos complexos compostos por activos físicos e cibernéticos heterogéneos e interligados, propriedade de diferentes IC nacionais, comunitárias e internacionais, que asseguram a troca rápida e sem descontinuidades de produtos/dados desde o produtor até ao consumidor final durante a prestação destes serviços.

A interligação dos activos físicos e cibernéticos expõe o ecossistema marítimo a **ameaças híbridas**, em que os ataques aos activos físicos se propagam aos activos cibernéticos e vice-versa.

Os ataques aos serviços da cadeia de abastecimento marítimo causam não só a interrupção dos serviços, mas também enormes danos às operações marítimas, à segurança internacional, às economias, às sociedades e ao ambiente. Por exemplo, os ataques aos sistemas de controlo industrial (ICS) (por exemplo, controlo de supervisão, SCADA, sistemas de controlo distribuído e controladores lógicos programáveis) alojados em portos ou empresas de transporte marítimo podem causar perturbações ou danos em dispositivos mecânicos críticos (por exemplo, gruas de contentores, sistemas mecânicos e de segurança que operam eclusas e barragens) e, pior ainda, podem causar a perda de vidas, o roubo de carga ou a destruição de um navio. Os efeitos (em termos de radiação térmica, onda de explosão de sobrepressão e estilhaços) da explosão de um navio-tanque de GNL ou nas instalações ou terminais de armazenamento de GNL dos portos, devido a um sistema SCADA pirateado, podem levar à perda de reservas de energia, o que pode ser crítico durante o inverno. Poderá também ter um impacto negativo no ambiente (degradação, fragmentação ou perda de ecossistemas), na economia e, mais importante ainda, no bem-estar e na saúde dos cidadãos. Um ataque a um sistema de gestão de terminais de contentores pode perturbar os serviços intermodais de contentores que envolvem o transporte marítimo, ferroviário e por camião.

Os ciberataques (por exemplo, a inserção de um programa malicioso) nos sistemas SCADA dos portos podem provocar derrames de combustível que afectam a qualidade da água; os ataques ao PCS podem transformar os navios-tanque de GNL em bombas flutuantes; os ataques físicos (por exemplo, bombardeamento) numa zona de armazenagem de produtos carboníferos a granel seco podem criar e transportar poeiras pelo vento para os terminais turísticos ou para as residências próximas. Os modernos sistemas de vigilância, unidades de monitorização, sensores, RFID, sistemas de tráfego marítimo, PCS, sistemas automatizados de controlo de fronteiras são susceptíveis às ameaças actuais. São propensos a espionagem, interrupção, vandalismo e interceção, o que pode causar a perturbação de várias operações e serviços marítimos críticos, bem como a sua utilização no tráfico de seres humanos e de droga e no terrorismo. Note-se que, de acordo com estimativas de 2016 da RAND Corporation e do Serviço de Investigação do Congresso dos EUA, um ataque a uma IC portuária poderia causar dezenas de milhares de mortes e paralisar o comércio global, com perdas que variam entre 45 mil milhões de dólares e mais de 1 trilião de dólares.

Em 2015, a Associação Internacional de Sistemas Comunitários Portuários recomendou que todos os actores marítimos, logísticos, da cadeia de abastecimento e operadores de SCP - com o apoio das suas associações comerciais e organismos internacionais e regionais - abordassem as actuais ameaças à cadeia de abastecimento. Além disso, recomendou que se reunissem as principais partes interessadas da cadeia de abastecimento para criar um Centro de Análise e Partilha de Informações (ISAC) para debater as ameaças, os riscos e as experiências em matéria de cibersegurança.

A ENISA publicou as ameaças mais importantes à cadeia de abastecimento, apresentadas de seguida [29]

FORNECEDOR	
Técnicas de ataque utilizadas para comprometer a cadeia de abastecimento	Activos dos fornecedores visados pelo ataque à cadeia de abastecimento
Infeção por malware	Software pré-existente
Engenharia social	Bibliotecas de software
Ataque de força bruta	Código
Exploração de vulnerabilidades de software	Configuração
Exploração de vulnerabilidades de configuração	Dados
Informações de fonte aberta (OSINT)	Processos
	Hardware
	Pessoas
	Fornecedor

CLIENTE	
Técnicas de ataque utilizadas para comprometer o cliente	Activos do cliente visados pelo ataque à cadeia de abastecimento
Relação de confiança [T1199]	Dados
Compromisso drive-by [T1189]	Dados pessoais
Phishing [T1566]	Propriedade intelectual
Infeção por malware	Software
Ataque físico ou modificação	Processos
Contrafação	Largura de banda
	Financeiros
	Pessoal

Figura 7: Taxonomia proposta pela ENISA para os ataques à cadeia de abastecimento.

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

É composto por quatro partes: (i) técnicas de ataque utilizadas no fornecedor, (ii) activos atacados do fornecedor, (iii) técnicas de ataque utilizadas no cliente, (iv) activos atacados do cliente.

4.4.2.5. Vectores de ameaça

Com base em vários recursos[30, 31, 32, 33, 34 e 35] as ameaças habituais à cibersegurança marítima e os bens marítimos visados por técnicas específicas são enumerados a seguir:

Ameaças	Técnicas	Activos e serviços marítimos como alvos
Ransomware	Acesso Inicial	Pessoas, sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, informações e dados, etc.
	Execução	Sistemas informáticos, dispositivos finais informáticos Componentes de rede e de comunicação, etc.
	Persistência	Pessoas, serviços de autoridade, serviços de apoio, etc.
	Elevação de privilégios	Pessoas, sistemas informáticos, dispositivos finais informáticos, etc.
	Evasão da defesa	Sistemas informáticos, dispositivos finais informáticos Componentes de rede e de comunicação, infra-estruturas móveis, infra-estruturas fixas, etc.
	Acesso às credenciais	Pessoas, sistemas informáticos, dispositivos finais informáticos, etc.
	Descoberta	Pessoas, sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, etc.
	Movimento Lateral	Pessoas, sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, informações e dados, etc.
	Coleção	Informações e dados, serviços de atracação de navios, serviços de segurança, pessoas, serviços de apoio, serviços de armazenamento temporário e de estadia Serviços de distribuição e de transferência, etc.
	Comando e controlo	Sistemas de TI, dispositivos finais de TI, componentes de rede e comunicação, informação e dados, serviços de atracação de navios, serviços de carga e descarga de navios, serviços de distribuição e transferência, infra-estruturas móveis, infra-estruturas fixas, sistemas e redes de TO, etc.
	Exfiltração	Dispositivos finais de TI, sistemas de TI, componentes de rede e de comunicação, sistemas e redes de TO, etc.
	Impacto	Sistemas de TI, dispositivos finais de TI, componentes de rede e comunicação, informações e dados, etc.
Malware	Violação da segurança	Dispositivos finais de TI, sistemas de TI, informações e dados, 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)

Engenharia social	Reconhecimento	Pessoas, sistemas informáticos, serviços das autoridades, serviços de segurança, sistemas de segurança, etc.
	Desenvolvimento de recursos	Pessoas, sistemas informáticos, serviços das autoridades, sistemas de segurança, informações e dados, etc.
	Acesso inicial	Pessoas, sistemas informáticos, sistemas e redes de TO, dispositivos finais informáticos, dispositivos finais de TO, etc.
	Execução	Pessoas, sistemas informáticos, etc.
Ameaças contra a disponibilidade (DDoS)	Desenvolvimento de Recursos	Sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, informação e dados, infra-estruturas móveis, infra-estruturas fixas, etc.
	Evasão de Defesas	Sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, etc.
	Impacto	Sistemas informáticos, dispositivos finais informáticos, componentes de rede e de comunicação, informação e dados, infra-estruturas móveis, infra-estruturas fixas, serviços de atracação de navios, serviços de carga e descarga de navios, serviços de distribuição e transferência, serviços de apoio, serviços de autoridades, serviços de segurança, etc.
Ameaças contra a disponibilidade (Ameaças na Internet)	Acesso Inicial	Dispositivos finais de TI, sistemas de TI, componentes de rede e de comunicação, etc.
	Descoberta	Dispositivos finais de TI, sistemas de TI, componentes de rede e de comunicação, etc.
	Coleção	Dispositivos finais de TI, sistemas de TI, componentes de rede e de comunicação, etc.
	Impacto	Dispositivos finais de TI, sistemas de TI, componentes de rede e de comunicação, etc.
Desinformação - Misinformação	Reconhecimento	Pessoas, dispositivos informáticos finais, sistemas informáticos, informações e dados, etc.
	Desenvolvimento de Recursos	Pessoas, dispositivos informáticos finais, sistemas informáticos, informações e dados, etc.
	Acesso Inicial	Pessoas, dispositivos informáticos finais, sistemas informáticos, etc.
	Execução	Pessoas, dispositivos informáticos finais, sistemas informáticos, etc.
	Impacto	Pessoas, dispositivos informáticos finais, sistemas informáticos, etc.
Ataques à cadeia de abastecimento	Reconhecimento	Tanto fornecedores como clientes (Quadro do cenário de ameaças para ataques à cadeia de abastecimento)
	Desenvolvimento de Recursos	Tanto fornecedores como clientes (Quadro do cenário de ameaças para ataques à cadeia de abastecimento)
	Acesso Inicial	Tanto fornecedores como clientes (Quadro do cenário de ameaças para ataques à cadeia de abastecimento)

5. Normas e estratégias de proteção do transporte marítimo

No presente capítulo, são apresentados os organismos de normalização e os órgãos políticos e são descritas as normas de proteção do transporte marítimo (segurança e cibersegurança) e o seu objetivo.

5.1. Introdução

Durante mais de uma década, foram envidados esforços significativos na introdução de metodologias de gestão e garantia dos riscos para as ICI, concentrando-se quer nas ciberameaças quer nas ameaças físicas, ignorando a complexa natureza dupla (física e cibernética) das ICI marítimas. No presente capítulo, são resumidas as normas de proteção do transporte marítimo pertinentes e, na última secção, são dadas orientações sobre o que utilizar para cada ameaça.

5.1.1. Estratégia Europeia de Segurança Marítima (EUMSS)

A primeira Estratégia de Segurança Marítima foi adoptada em 24 de junho e 16 de dezembro de 2014 como resposta aos riscos e ameaças modernos à segurança marítima mundial. A estratégia promove uma melhor cooperação e coordenação civil-militar entre os intervenientes na segurança interna e externa, como a polícia e a defesa. O objetivo é que esta abordagem conjunta da segurança marítima promova uma cooperação mais estreita entre os diferentes sectores marítimos e torne a política de segurança marítima da UE mais coerente, eficaz e eficiente em termos de custos. Este conjunto de ferramentas explica como o plano de ação deve ser aplicado e destaca as actividades do Serviço Europeu para a Ação Externa (SEAE) e o papel das delegações da UE e dos serviços centrais do SEAE.

A Estratégia de Segurança Marítima da UE revista, adoptada em junho de 2018, permite um processo de apresentação de relatórios mais específico para aumentar a sensibilização e um melhor acompanhamento da primeira estratégia. O plano de ação reúne os aspectos internos e externos da segurança marítima da União, facilita uma abordagem estratégica e intersectorial e estabelece uma agenda conjunta civil-militar para a investigação sobre segurança marítima (incluindo a dupla utilização).

A estratégia revista sublinha que deve ser assegurada uma melhor coordenação na aplicação das estratégias e políticas da UE com objectivos transversais, como as que se referem aos domínios da energia, do ambiente e das ameaças e desafios à segurança, incluindo as ameaças cibernéticas e híbridas, o terrorismo e a criminalidade organizada. Salienta a natureza evolutiva das ameaças no domínio marítimo e apela a um empenhamento renovado na proteção das infra-estruturas marítimas críticas, incluindo as subaquáticas, e das infra-estruturas de transporte marítimo, de energia e de comunicações, nomeadamente através do reforço do conhecimento marítimo através de uma melhor interoperabilidade e de um intercâmbio de informações simplificado (obrigatório e voluntário). Apela à melhoria da proteção e da resiliência dos sistemas e infra-estruturas marítimas. A este respeito, são consideradas as políticas e iniciativas comunitárias pertinentes.

Uma das principais acções mencionadas é o ponto A.3.8 revisto: "Melhorar a integração de uma dimensão de cibersegurança no domínio marítimo em termos de capacidades, investigação e tecnologia e indústria, com base na coordenação civil-militar e nas sinergias com as políticas da UE em matéria de cibersegurança e ciberdefesa, em conformidade com a Diretiva SRI e com as recomendações e regulamentações internacionais, como a SOLAS XI-2 e o Código ISPS e as suas futuras actualizações. Tal incluirá o intercâmbio de melhores práticas e o desenvolvimento de projectos conjuntos pelos Estados-Membros da UE sobre a prevenção de ciberataques marítimos."

A ação A.4.3 indica: "Prosseguir uma abordagem global da gestão dos riscos para a proteção do transporte marítimo, nomeadamente através de uma análise comum dos riscos e da identificação de eventuais lacunas e sobreposições neste domínio, tendo igualmente em conta as ciberameaças e as ameaças híbridas, os desafios climáticos e as catástrofes ambientais marítimas."

A ação A.4.8 indica que: "Desenvolver uma rede de peritos em cibersegurança e ciberdefesa no domínio marítimo para elaborar orientações sobre procedimentos em resposta a ameaças emergentes no domínio marítimo, incluindo possíveis actos de terrorismo e outros actos ilícitos intencionais no mar, especialmente no que diz respeito à proteção de navios, carga, tripulação e passageiros, portos e instalações portuárias, instalações de energia marinha e outras infra-estruturas marítimas e energéticas críticas, em conformidade com a Diretiva SRI e o Código ISPS." O desenvolvimento de capacidades e o reforço do ensino e da formação em matéria de cibersegurança no domínio marítimo, em colaboração com todas as partes interessadas (por exemplo, a ONU, a Organização Internacional do Trabalho (OIT), a OMI e a NATO), também fazem parte das acções da estratégia revista (acções A.5.1 e A.5.6).

A EUMSS abrange os aspectos internos e externos da proteção marítima da União e contribui para um domínio marítimo mundial estável e seguro, em conformidade com a Estratégia Europeia de Segurança. A Direção-Geral (DG) MARE é o organismo da Comissão Europeia responsável pelo desenvolvimento da estratégia, com a colaboração de várias DG (por exemplo, DG CNECT, DG MOVE, DG ECHO, DG RTD) e agências (por exemplo, Agência Europeia da Segurança Marítima (EMSA), ENISA). A Estratégia da União Europeia para a Segurança 2020 promove a autonomia estratégica e a resiliência das cadeias de abastecimento da UE em termos de produtos, serviços, infra-estruturas e tecnologias críticos.

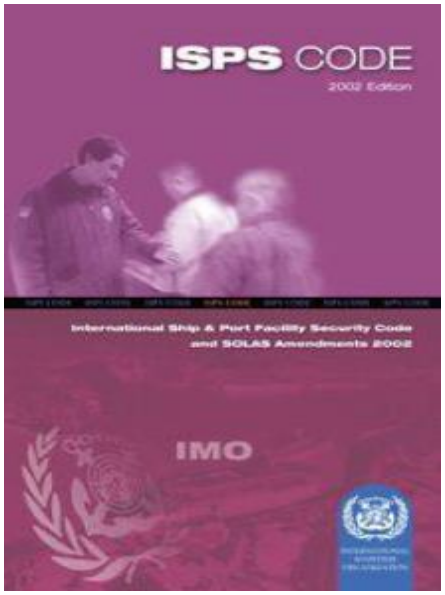
5.1.2. Normas de segurança marítima

As organizações marítimas (e.g., IMO, BIMCO, EMSA) emitiram várias normas e directrizes relacionadas com a segurança, algumas das quais são a seguir descritas.

5.1.2.1. O Código ISPS

mais importante é o Código Internacional para a Segurança dos Navios e das Instalações Portuárias (ISPS) da OMI, que é o código internacional para a segurança dos navios e das instalações portuárias, estabelecido pela OMI, no âmbito da Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS) 1974 (capítulo XI-2).[35]

[35] (SOLAS XI-2 e o Código Internacional de Protecção de Navios e Instalações Portuárias (ISPS), s.d.)



O Código ISPS estabelece um quadro através do qual os navios e as instalações portuárias podem cooperar na deteção e dissuasão de actos que constituam uma ameaça à proteção do transporte marítimo. O código prevê uma abordagem para estabelecer uma governação da segurança nas IC marítimas. O código:

- permite a deteção e dissuasão de ameaças à segurança num quadro internacional;
- estabelece funções e responsabilidades;
- permite a recolha e o intercâmbio de informações em matéria de segurança;
- fornece uma metodologia para avaliar a segurança;
- garante a adoção de medidas de segurança adequadas.

O código é composto por duas partes, que contêm prescrições obrigatórias e directrizes para a proteção dos navios e das instalações portuárias. A Parte A contém as prescrições obrigatórias e a Parte B as recomendações de aplicação para reforçar a proteção. Neste contexto, os princípios subjacentes ao Código ISPS são semelhantes aos do Código ISM a bordo de um navio. Antes de o Código ISPS ser legalmente aplicável num país, tem de ser transposto para a legislação nacional. Alguns países adoptaram o Código ISPS pouco depois de julho de 2004, mas outros só o fizeram anos mais tarde. Alguns países adoptaram o código na íntegra e outros introduziram alterações ao código ISPS nacional no que respeita a determinados aspectos da segurança portuária.

A União Europeia[36] aplicou de imediato a Parte A do código nos seus portos e decidiu considerar também a Parte B como obrigatória e não como mera recomendação. Os países africanos aplicaram o código de forma independente, através da sua legislação nacional.

É importante sublinhar que o Código ISPS utiliza a palavra "instalação portuária", o que significa que o porto não está abrangido pelo ISPS. Os aspectos de segurança "portuária" são abordados no Código de Conduta para a Segurança nos Portos (COP).

[36] Diretiva 2005/65/CE relativa ao reforço da segurança nos portos e zonas adjacentes

O Código de Conduta de Genebra de 2003 relativo à segurança portuária complementa as disposições do Código ISPS no que respeita à garantia da segurança da zona portuária em geral. O código define funções, deveres e medidas de segurança para dissuadir e reagir a actos criminosos contra os portos. Utiliza as mesmas práticas e princípios que o Código ISPS e constitui um guia para toda a segurança portuária para além da zona das instalações portuárias. A União Europeia introduziu o código como uma diretriz obrigatória[37] para melhorar a segurança dos seus portos.

5.1.2.1.1. Segurança na construção

A partir do momento em que um navio é construído, a segurança começa com o requisito de que um navio esteja em condições de navegar antes de deixar a costa, conforme exigido pelo Lloyds of London (P&I Club)[38]. Cada navio mercante é registado por um Estado de bandeira, quer se trate do país de residência do armador ou de um país que arvore uma bandeira de conveniência. Devem cumprir as regras, regulamentos e disposições marítimas do Estado de bandeira específico, em conformidade com as regras e disposições marítimas internacionais da OMI, e devem ser certificados por uma sociedade de classificação.

No entanto, alguns pavilhões de conveniência têm uma segurança reduzida, não dispõem de recursos adequados para efetuar inspecções correctas e não impõem sanções aos navios em infração. Esta situação resulta em navios que não cumprem vários requisitos críticos de segurança, mas que por vezes continuam a ser autorizados a atracar em determinados portos. Uma vez que estes navios inseguros se limitam a reparar partes do navio quando este apresenta defeitos, em vez de se concentrarem na manutenção preventiva, o risco de acidente é elevado.

5.1.2.1.2. Controlo do Estado do Porto (PCS)

É da responsabilidade do Estado de bandeira (o país onde o navio está registado) garantir que um navio cumpre todas as normas de segurança exigidas. O PSC funciona como um apoio eficaz às inspecções que são efectuadas regularmente pelos Estados de bandeira para detetar navios que não cumprem as normas.

O PSC é, portanto, a iniciativa de segurança marítima (proteção física) da IMO que tem por objetivo verificar a conformidade de um navio com as convenções e normas internacionais. Contribui para reduzir o risco de perigos para os navios. O papel do PSC é chamar a atenção para os potenciais riscos de proteção (segurança e cibernética) e comunicá-los ao Estado de bandeira do navio. Durante as inspecções dos navios, o PSC verifica se o estado do navio e o seu equipamento de movimentação cumprem os requisitos dos regulamentos internacionais da OMI e se o navio é tripulado e operado em conformidade com essas regras. Trabalham de acordo com uma resolução de cooperação para o controlo dos navios e das descargas (Resolução 682 17 da OMI).[39]

[37] Diretiva 2005/65/CE relativa ao reforço da segurança nos portos e zonas adjacentes
[38] (Rulebook 2021)
[39] (Resolução A.682 (17), 1991)

5.1.2.1.3. Normas de operações de segurança dos navios

Os marítimos são o fator humano que pode reduzir os riscos a bordo. Este papel é desempenhado pelo responsável pela segurança a bordo, que é nomeado para manter atualizado o plano de gestão da segurança, utilizar um sistema de gestão da segurança (SMS) e manter a tripulação alerta através de formação em matéria de segurança. A espinha dorsal da governação da segurança é o SGS, uma vez que o seu principal objetivo é fornecer uma abordagem sistemática para a gestão dos riscos de segurança nas operações do navio. O SGS faz parte do Código Internacional de Gestão da Segurança (ISM)[40] e os navios comerciais são obrigados pela OMI a estabelecer procedimentos de gestão segura dos navios.

Um dos aspectos mais importantes para manter a integridade do navio durante uma viagem marítima é ter a carga bem acondicionada. As forças laterais e longitudinais sobre o navio criadas pela ondulação durante as tempestades constituem um enorme risco para a estabilidade do navio devido aos riscos de deslocação da carga. Toda a carga deve ser estivada e acondicionada de modo a não pôr em risco o navio e a tripulação. Devem ser seguidos procedimentos correctos de amarração e fixação, em conformidade com o código CSS da OMI[41]. Se um ataque malicioso fizer com que a carga não esteja segura e se desloque livremente no porão, o risco de perder o navio e a tripulação é real.

5.1.2.1.4. Aspectos de segurança curativa a bordo dos navios

No caso de ocorrer um acidente a bordo, é vital que a tripulação seja treinada para minimizar imediatamente o impacto dos danos causados. Por conseguinte, os membros da tripulação recebem formação sobre os princípios de gestão de crises e os procedimentos de resposta de emergência a todos os tipos de acidentes e sobre como combater um incêndio. O Código de Formação, Certificação e Serviço de Quartos dos Marítimos (STCW)[42] e a Convenção SOLAS abordam estes aspectos em pormenor, mas este domínio de especialização está fora do âmbito do presente estudo.

5.1.2.2. Outros códigos importantes

- Código Marítimo Internacional para o Transporte de Cargas Sólidas a Granel (Código IMSBC) da OMI;
- Código Internacional para a Construção e o Equipamento dos Navios que Transportam Produtos Químicos Perigosos a Granel (Código IBC)
- Código Internacional para a Segurança do Transporte de Cereais a Granel (Código Internacional dos Cereais);
- Código de Práticas para a Segurança das Operações de Carga e Descarga de Navios Graneleiros (Código BLU);
- Código Marítimo Internacional para o Transporte de Mercadorias Perigosas (IMDG);

[40] (Código Internacional de Gestão para a Segurança (ISM))
[41] (Code of Safe Practice for Cargo Stowage and Securing (CSS Code), s.d.)
[42] (Convenção Internacional sobre Normas de Formação, de Certificação e de Serviço de Quartos para os Marítimos, 197, s.d.)

- A EMSA[43] disponibiliza ferramentas para as partes interessadas do sector marítimo da UE, por exemplo, AIS, SafeSeaNet para monitorização do tráfego de navios, imagens de satélite CleanSeaNet para identificação da poluição no mar, EMCIP para centralização de dados sobre acidentes marítimos, ferramentas de formação, etc.
- A Organização Europeia dos Portos Marítimos[44] promove os portos verdes e os esforços de eficiência energética e é especializada em orientações de segurança e formação relacionadas com as operações dos navios nos portos, por exemplo: Abastecimento de GNL, receção de resíduos, carga e descarga de mercadorias em geral, contentores e granéis, e movimentos de contentores.
- A OIT[45] publicou o código de práticas da OIT sobre segurança e saúde nos portos; o código da OIT fornece orientações relevantes para a gestão, operação, manutenção e desenvolvimento dos portos.
- A Iniciativa de Segurança de Contentores (CSI) da USC
- Parceria Comercial Aduaneira contra o Terrorismo (CTPAT)
- Plano de segurança da tripulação
- Sistema de Manifesto Automatizado (AMS)
- SafeSeaNet
- AIS

5.1.3. Normas de cibersegurança

5.1.3.1. ISO[46] snormas para a proteção das ICI marítimas

A norma ISO27000 apresenta definições de conceitos de segurança. A ISO/IEC 27001 aborda os requisitos de segurança física em termos de prevenção do acesso não autorizado à informação de uma organização e das suas instalações relevantes, que se dividem em duas grandes categorias: áreas seguras e segurança do equipamento.

A norma ISO/IEC 27001 trata igualmente do Sistema de Gestão da Segurança da Informação (SGSI) de uma organização que, no caso do presente relatório, é o CII do porto. A conformidade com a norma ISO 27001 significa praticamente que a organização, no nosso caso o porto, cumpre os requisitos da norma no domínio da segurança, o que é vital para o bom funcionamento do porto num ambiente de segurança contra as ameaças do ciberespaço. As ICI estão bem protegidas. Além disso, a norma clarifica os termos de segurança física, como o perímetro de segurança física, os controlos físicos à entrada e as instalações. Os requisitos de segurança física também são identificados na publicação especial 800-171 do NIST. A família de normas ISO2800x fornece directrizes para a segurança da cadeia de abastecimento

[43] (Agência Europeia da Segurança Marítima, s.d.)
[44] (ESPO: The First Port of Call for European Transport Policy Makers in Brussels, s.d.)
[45] (OIT: Organização Internacional do Trabalho, s.d.)
[46] (Normas, s.d.)

e, em especial, para as cadeias de abastecimento marítimas. O quadro seguinte[47] resume as várias normas ISO que são relevantes para a proteção do transporte marítimo.

R/N	ISO	COMENTÁRIOS
1.	ISO 18788:2015	Sistema de gestão para operações de segurança privada
2.	ISO 9001 / BS 10800	Código de conduta para a prestação de serviços de segurança
3.	ISO/IEC 27001	Norma internacional para gerir a segurança da informação
4.	ISO 27002:2013 (previous ISO 17799:2000)	Norma abrangente de segurança da informação. É composta por catorze secções (5 a 18), cada uma das quais está estruturada da mesma forma
5.	ISO/IEC TS 30104:2015	Tecnologia da informação - Técnicas de segurança - Ataques à segurança física, técnicas de atenuação e requisitos de segurança
6.	ISO 28000:2007	Especifica os requisitos de um sistema de gestão da segurança, incluindo os aspectos críticos para a garantia da segurança da cadeia de abastecimento
7.	ISO 28000:2022	Segurança e resiliência - Sistemas de gestão da segurança - Requisitos

Uma vez que os navios autónomos e as aplicações marítimas inovadoras utilizam a IA, é necessário ter em conta várias normas adicionais para o desenvolvimento de um ecossistema marítimo fiável baseado na IA.

As principais normas para a IA são mencionadas a seguir:

5.1.3.2. Normas ISA, ANSI para ACS

As normas ISA e ANSI destinam-se à segurança dos sistemas de automação e controlo industrial (ACS, por exemplo, SCADA). Exemplos de tais normas incluem:

- ISA-TR62443-2-3-2015 Segurança para sistemas de controlo e automação industrial, Parte 2-3: Gestão de patches no ambiente IACS
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 Segurança para sistemas de controlo e automação industrial, Parte 2-4: Requisitos do programa de segurança para fornecedores de serviços IACS (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020 Segurança para sistemas de automação e controlo industrial, Parte 3-2: Avaliação do risco de segurança para a conceção do sistema
- ANSI/ISA-62443-4-1-2018 Segurança para sistemas de controlo e automação industrial, Parte 4-1: Requisitos do ciclo de vida do desenvolvimento de produtos seguros

[47] Y. Papagiannopoulos, "Standards in Practice", Conferência do IEEE sobre normas para comunicações e redes, novembro de 2022

5.1.3.3. Categorização das normas

Há muitas normas de segurança de vários organismos de normalização (por exemplo, ISO, IMO, ETSI, NIST, BIMCO, IEEE) que abordam vários temas. Esta fragmentação de esforços gera confusão quanto à(s) norma(s) a utilizar. É necessário clarificar as complementaridades e sobreposições. Para contribuir para esta clarificação, foi apresentada uma classificação das normas[48], tendo sido identificadas as seguintes dez categorias de normas:

1. Vocabulário e concetualização: normas que podem ser utilizadas para definir terminologias e descrição de conceitos.
2. Requisitos de segurança: normas que estabelecem requisitos de segurança.
3. Directrizes de segurança: normas que fornecem boas práticas.
4. Avaliação e apreciação da segurança: normas e boas práticas relacionadas com a apreciação ou metodologias de avaliação da segurança.
5. Privacidade e proteção de dados: normas relacionadas com a manutenção da privacidade e a proteção de dados.
6. Normas de gestão dos riscos: normas e boas práticas que fornecem princípios, quadros ou processos relacionados com a gestão dos riscos de segurança.
7. Normas técnicas: normas que abordam aspectos técnicos de segurança.
8. IA e segurança: Inclui normas, quadros e boas práticas relacionadas com a segurança da IA (importante para as embarcações autónomas, afogamentos marítimos).
9. Sector específico (ou seja, transporte marítimo): normas de gestão da segurança que apoiam os requisitos específicos e as especificidades do sector específico (por exemplo, sistemas portuários comunitários).
10. Proteção das infra-estruturas críticas: normas relacionadas com a proteção das infra-estruturas que são críticas para a sustentabilidade da economia e o bem-estar social (por exemplo, as ICI marítimas).

[48] (Kalogeri & Polemi, 2022)

Figura 8: Taxonomia das normas de segurança marítima[49]

5.2. Legislação de segurança

A regulamentação da segurança nos portos de todo o mundo (incluindo os africanos) não é, em princípio, totalmente regulada pelas normas internacionais e continua a ser uma decisão do Estado soberano. Cada país estabeleceu os seus próprios regulamentos de segurança, o que produziu uma carteira variada de leis por vezes diferentes e desactualizadas.

Os princípios de segurança da governação portuária são fundamentais, uma vez que envolvem muitos decisores e partes interessadas, como a autoridade portuária, os operadores de terminais, os operadores ferroviários, as empresas de camionagem, os fornecedores de logística e os serviços de emergência. Os aspectos gerais de segurança na zona portuária, mas também os aspectos de segurança da movimentação da carga, devem ser tidos em conta no desenvolvimento de um sistema de gestão da segurança portuária. Não seria possível fazer justiça ao assunto aqui, mas um fator comum é que a segurança deve abranger infra-estruturas e equipamento de movimentação de qualidade, pessoal bem treinado, um conjunto de procedimentos bem pensados e um SGS que monitorize e acompanhe a situação real de segurança. É da responsabilidade do responsável pelo porto e pelas instalações gerir o seu SGS de forma profissional para evitar danos ou prejuízos para as pessoas. O escudo de segurança não deve tornar-se frágil, permitindo danos consequentes de ciberataques ou ataques à segurança.

[49] *Ibid.*

A maior parte da legislação no mundo marítimo foi iniciada por algum desastre marítimo e, neste caso, o desastre do Titanic levou à adoção da regulamentação internacional de segurança SOLAS de 1974 como "escudo de segurança" protetor para os marítimos e os

navios. A extensa cobertura mediática, o subsequente choque global causado pelo enorme número de mortos e a ação judicial dos sobreviventes contra a White Star Line conduziram a melhorias significativas na segurança marítima.

Para além desta pressão social, as companhias de seguros marítimos forçaram as empresas de navegação a mostrar mais liderança na prevenção de acidentes e convenceram os governos a estabelecer leis de segurança mais eficazes. Passou-se de uma atitude de fuga aos factos e de pagamento de indemnizações para uma mentalidade de sensibilização para a segurança e de prevenção, que é vital para a proteção dos seres humanos, mais barata para as companhias de seguros e mais eficiente para os armadores. O mundo marítimo continua a ser um sector de alto risco, com enormes consequências quando algo corre mal.

A melhoria mais importante foi a criação da Convenção SOLAS, que estabelece princípios e regras uniformes para a construção, instalação e funcionamento dos navios mercantes. A atual versão da Convenção SOLAS de 1974[50] continua a ser a norma mundial para os navios e os marítimos. Cada país, cada porto e cada situação local são diferentes e exigem uma abordagem de risco complexa e personalizada para todas as operações, a fim de atenuar e minimizar os riscos de segurança. Alguns países, como a Austrália, promovem a abordagem personalizada de liderança em matéria de segurança nos portos e limitam-se a fornecer orientações sobre boas práticas e a delinear um modelo com base no qual as políticas, os procedimentos e o desempenho das operações portuárias podem ser avaliados.

Como cada porto tem os seus riscos de segurança únicos, as regras de gestão da segurança só podem ser abordadas a partir do próprio porto e utilizar os regulamentos, directrizes e melhores práticas internacionais como uma ferramenta para melhorar a segurança no porto. No mundo atual, não é possível criar uma regulamentação internacional única e uniforme em matéria de segurança, especialmente porque alguns países não dispõem sequer dos princípios básicos de segurança.

Mas, ao contrário deste regulamento de segurança, a criação de uma "legislação de segurança" foi desencadeada por uma catástrofe em terra, quando aviões sequestrados embateram nas torres gémeas do World Trade Centre em 11 de setembro de 2001.

Atualmente, o sector marítimo é controlado por vários regulamentos que exigem que os operadores marítimos garantam a segurança e a proteção dos navios. Estes regulamentos aplicam-se igualmente à cibersegurança e à Resolução MSC.428(98) da IMO. Os riscos de cibersegurança devem agora ser abordados no sistema de gestão da segurança (SMS). De acordo com as Directrizes de Gestão do Risco Cibernético Marítimo da OMI (MSC-FAL.1 Circ.3)[51], "...o risco cibernético marítimo refere-se a uma medida do grau em que uma

[50] (Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS), 1974, s.d.)
[51] (Guidelines on Maritime Cyber Risk Management, 2017)

instalação tecnológica é ameaçada por uma circunstância ou evento potencial, que pode resultar em falhas operacionais, de segurança ou de proteção relacionadas com o transporte marítimo devido a danos, perda ou comprometimento dos sistemas de informação".

Para além das orientações da OMI, a Associação Internacional de Portos e Portos (IAPH) também elaborou um conjunto de orientações de cibersegurança para portos e instalações portuárias[52].

Alguns dos regulamentos europeus específicos em matéria de segurança portuária são os seguintes:

- Diretiva 2000/59/CE do Parlamento Europeu e do Conselho, de 27 de novembro de 2000, relativa aos meios portuários de receção de resíduos gerados em navios e de resíduos da carga.
- Diretiva 2001/96/CE do Parlamento Europeu e do Conselho, de 4 de dezembro de 2001, que estabelece normas e procedimentos harmonizados para a segurança das operações de carga e descarga de navios graneleiros.
- Diretiva 2000/59/CE do Parlamento Europeu e do Conselho, de 27 de novembro de 2000, relativa aos meios portuários de receção de resíduos gerados em navios e de resíduos da carga.Cybersecurity Legislation

5.3. Legislação sobre cibersegurança

A UE adoptou e reforçou o Código ISPS através de duas directivas - a CE/725/2004 para as instalações portuárias e a CE/65/2005 para os portos. A UE está a proteger as suas infra-estruturas (incluindo as ICI marítimas) através de vários instrumentos jurídicos, nomeadamente

A *Diretiva SRI* estabeleceu uma competência europeia em matéria de cibersegurança para proteger o mercado único digital; tem três objectivos principais: a) melhorar as capacidades nacionais de cibersegurança, exigindo que todos os Estados-Membros tenham um conjunto mínimo comum de capacidades de base. b) Facilitar a cooperação transfronteiras a nível da UE entre os Estados-Membros e a União, tanto a nível estratégico/político como operacional, em matéria de cibersegurança. Isto envolve tanto o Grupo de Cooperação SRI como a Rede de CSIRTs. e c) promover uma cultura de gestão dos riscos e de comunicação de incidentes entre os principais agentes económicos, nomeadamente os operadores que prestam serviços essenciais (OES) para a manutenção das actividades económicas e sociais e os prestadores de serviços digitais (DSP).

O *Ato para a Cibersegurança da UE* estabelece um quadro de certificação da cibersegurança para produtos e serviços. Este quadro proporcionará sistemas de certificação à escala da UE como um conjunto abrangente de regras, requisitos técnicos, normas e procedimentos. Desta forma, será possível garantir a confiança do público na cibersegurança dos produtos e serviços informáticos. É importante que se possa demonstrar que um produto foi verificado e certificado em conformidade com normas elevadas de cibersegurança. Os produtos relacionados com a IA ganharão confiança se forem certificados e, nos próximos anos, serão

[52] (Measures to Enhance Maritime Security: IAPH Cybersecurity Guidelines for Ports and Port Facilities, 2021)

desenvolvidos vários regimes de cibersegurança para os produtos de IA, especificando os requisitos de segurança.

O *Regulamento Geral sobre a Proteção de Dados* (RGPD) estabelece regras de proteção de dados que explicam o que, como e quando as pessoas podem aceder às informações que lhes dizem respeito e impõe restrições ao que as organizações podem fazer com os dados pessoais.

O *Novo Quadro Legislativo* (NLF) melhora a fiscalização do mercado, introduz regras para proteger melhor os consumidores e os profissionais de produtos não seguros (UE ou não UE), estabelece regras para a acreditação e estabelece um quadro jurídico comum para os produtos industriais. O NLF reforçará a segurança dos produtos baseados na IA.

A *Lei dos Chips* é relevante para a segurança da IA porque os semicondutores são a tecnologia de plataforma do século XXI que será utilizada para o desenvolvimento da IA e para a incorporação de fortes medidas de segurança. A indústria globalizada de semicondutores da UE será apoiada por esta proposta de lei.

O *Ato para a Ciber-resiliência* estabelecerá, em tempo útil, novas regras de cibersegurança para os produtos digitais e os serviços auxiliares. Esta iniciativa promoverá também a segurança dos produtos de IA, uma vez que visa responder às necessidades do mercado e proteger os consumidores de produtos inseguros, introduzindo regras comuns de cibersegurança para os fabricantes e vendedores de produtos digitais corpóreos e incorpóreos.

6. Boas práticas de segurança marítima

6.1. Introdução

As IC marítimas (portos ou navios) devem ser consideradas infra-estruturas físico-cibernéticas.
Existem várias directrizes para a segurança das IC marítimas:

- **ENISA Boas práticas para a cibersegurança no sector marítimo** (2019)
- **ETSI TR 103 456** CYBER; Implementação do SRI **COM(2017) 476 final** "Tirar o máximo partido do SRI"
- **C(2017)6100 final** Recomendação sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (projeto)
- **Gestão/autoavaliação de navios-tanque - TMSA** (OCIMF)
- **Directrizes sobre cibersegurança a bordo dos navios** (apoiadas por: **BIMCO**, CLIA, **ICS**, INTERCARGO, INTERTANKO, OCIMF e IUMI)
- **Sensibilização para a cibersegurança** - AMMITEC

Este capítulo sublinha os passos que devem ser dados a nível pessoal, organizacional e operacional para enfrentar holisticamente os desafios da segurança. A segurança é considerada uma responsabilidade conjunta e todas as partes interessadas envolvidas devem adotar boas práticas de cibersegurança. Foram elaborados dois questionários (ver Anexos A e B) a distribuir futuramente aos operadores marítimos para avaliar o seu nível de sensibilização para a segurança.

6.2. Governação da segurança marítima

A higiene da segurança de uma IC marítima (por exemplo, porto, navio, companhia marítima) é parte integrante da estrutura global da IC. A higiene da segurança consiste em todas as acções que têm de ser tomadas para que a IC marítima possa funcionar com um nível de risco aceitável contra ameaças físicas, cibernéticas, híbridas e da cadeia de abastecimento. Para compreender melhor a higiene da segurança de uma IC marítima, é necessário começar por saber quem são as principais autoridades e partes interessadas envolvidas na estrutura global, nas operações, nos serviços e nos utilizadores internos e externos. É igualmente necessário identificar todos os activos físicos e cibernéticos da IC marítima, as suas interligações, a sua interação e a sua importância (valor) para as operações da IC. É necessário atribuir um proprietário a cada bem que será responsável pela sua segurança (um proprietário pode ser responsável por vários bens).

Uma IC marítima é um sistema de sistemas integrados numa única entidade. Para compreender melhor o ecossistema da IC, é necessário saber quem participa na gestão dos activos. Isto é importante, uma vez que indica a governação da segurança da informação de uma IC marítima e as medidas gerais de segurança que devem ser tomadas para proteger estes activos.

Todas as IC marítimas devem aplicar e praticar um esquema de governação da segurança da informação do seguinte modo:

- Políticas (obrigatório)
- Normas (obrigatórias)
- Directrizes (não obrigatórias)
- Procedimentos (obrigatório)
- Linhas de base (obrigatório)

As políticas, normas, directrizes e procedimentos estabelecem a governação da segurança de uma organização. A este respeito, a higiene da segurança de uma organização pode ser alcançada através da aplicação dos elementos da governação da segurança e do estabelecimento de um sistema de gestão da segurança da informação bem protegido i) baseado nos controlos de segurança adequados, ii) da aplicação dos controlos de segurança, iii) da avaliação dos controlos de segurança no ambiente marítimo que estão a ser aplicados e iv) da monitorização regular da sua eficácia. A higiene da segurança deve ser aplicada com base na abordagem de governação da segurança acima descrita.

A estrutura de governação tem de ser aplicada a ambos os aspectos da segurança (segurança e cibersegurança) numa abordagem uniforme e tem de ser parte integrante de todas as actividades de IC marítimas. Os procedimentos de governação devem incluir uma análise do impacto nas actividades (BIA), uma avaliação actualizada dos riscos e uma política de segurança. A este respeito, a governação da segurança da informação deve ser regularmente monitorizada e avaliada com base nos indicadores-chave de desempenho (KPI) e nos indicadores-chave de risco (KRI) da segurança física e cibernética e da segurança do pessoal. Uma equipa de tratamento de incidentes tem de fazer parte da equipa de governação da segurança, que será responsável pela previsão, identificação, análise, atenuação e recuperação de qualquer incidente de segurança (físico, cibernético, híbrido).

Deve ser criada uma autoridade central, com mandato para supervisionar a aplicação da governação da segurança da informação através da inspeção (controlo da segurança) do sistema global de segurança da IC marítima.

6.3. Higiene da cibersegurança dos operadores

Os dados do Relatório de Investigações de Violação de Dados (DBIR) de 2019 da Verizon indicam que quase um terço (32%) de todas as violações de dados envolveu esquemas de phishing.[53] Um novo site de phishing é lançado a cada 20 segundos, conforme mencionado no Relatório sobre o cenário de ameaças móveis de 2020, Wandera. O erro humano causou 90 por cento das violações de dados cibernéticos em 2019, de acordo com a análise de dados do Gabinete do Comissário da Informação do Reino Unido (ICO) realizada pela CybSafe. De acordo com esta análise, nove em cada 10 das 2376 ciberviolações comunicadas ao ICO no ano passado foram causadas por erros cometidos por utilizadores finais. Os ataques de phishing são responsáveis por mais de 80% dos incidentes de segurança comunicados; perdem-se 17 700 dólares por minuto devido a ataques de phishing; 60% das violações

[53] (Widup, 2019)

envolveram vulnerabilidades para as quais existia uma correção mas que não foi aplicada pelos administradores.

É necessário que todos os operadores marítimos e utilizadores individuais apliquem boas práticas de segurança pessoal, definindo as regras e envidando esforços para:

- Criar uma cultura de sensibilização para a segurança e a ciber-higiene
- Incentivar a partilha de informações e a colaboração
- Envolver os operadores e utilizadores nas decisões e procedimentos relacionados com a segurança
- Utilizar cartazes e lembretes
- Formação prática contínua em matéria de segurança a todos os níveis (de seminários a exercícios)
- Controlo de acesso eficaz
- Aplicar políticas de autenticação e de palavra-passe

6.4. Gestão da proteção marítima

A gestão dos riscos físicos, cibernéticos e híbridos exige uma abordagem holística. As medidas gerais que devem ser tomadas durante a gestão da proteção (segurança e cibersegurança) de uma IC marítima são as seguintes:

1) Identificar os activos (físicos e cibernéticos) e atribuir a propriedade, por exemplo, designar a(s) pessoa(s) que será(ão) responsável(eis) pelo ativo[54].
2) Criar um inventário de atualização dinâmica dos activos (listar a propriedade).
3) Categorizar e classificar os activos com base em:

- Valor do ativo (importância para a IC marítima);
- Importância do ativo no ecossistema marítimo global;
- Tipo de ativo (físico, cibernético, utilizador, procedimentos).

4) Identificar o cenário de ameaças e a superfície de ataque de cada ativo.
5) Selecionar e utilizar uma metodologia de avaliação dos riscos (por exemplo, a partir do inventário da ENISA) e estimar os riscos.
6) Tomar medidas para proteger os activos utilizando listas de controlos publicadas, por exemplo, ISO 27002, NIST2020, SANS Top 20, CIS e melhores práticas, e desenvolver o plano de tratamento dos riscos (plano de emergência).
7) Desenvolver a política de segurança com regras que regem a forma como os activos são geridos, protegidos e distribuídos na organização, utilizando os esforços existentes, por exemplo, ISPS, orientações BIMCO ou ISO/IEC PDTR 13335-1 (11/2001).
8) Identificar continuamente novas ameaças e incidentes, avaliar os riscos, a propriedade dos bens das ICI, a solidez dos controlos e a gestão dos incidentes e riscos

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

estimados.

9) Tomar medidas para proteger os activos utilizando listas de controlos publicadas, por exemplo, ISO 27002, NIST2020, SANS Top 20, CIS e melhores práticas, e desenvolver o plano de tratamento dos riscos (plano de emergência).

10) Desenvolver a política de segurança com regras que regem a forma como os activos são geridos, protegidos e distribuídos na organização, utilizando os esforços existentes, por exemplo, ISPS, orientações BIMCO ou ISO/IEC PDTR 13335-1 (11/2001).

11) Identificar continuamente novas ameaças e incidentes, avaliar os riscos, a propriedade dos bens das ICI, a solidez dos controlos e a gestão dos incidentes.

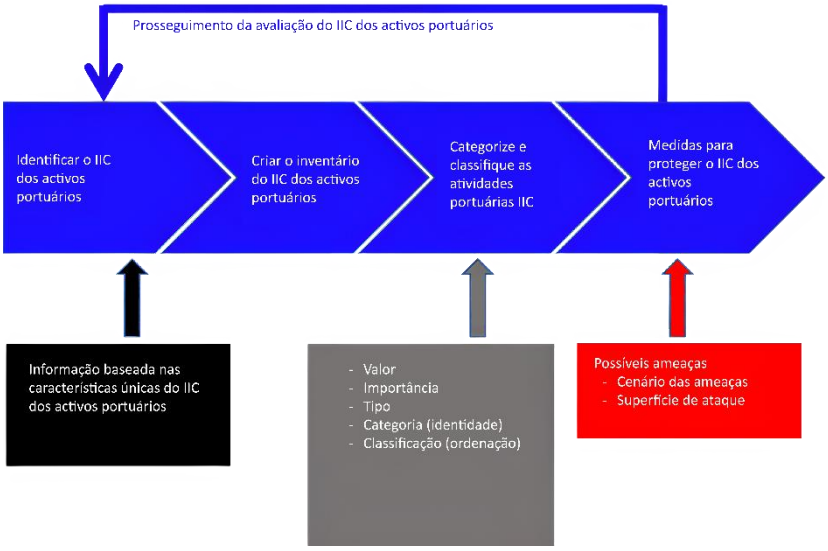


Figura 9: Abordagem da BIMCO à gestão da segurança

6.4.1. Gestão da segurança (segurança física)

Antes do incidente de 11 de setembro, os navios mercantes entravam tradicionalmente nas águas territoriais e nos portos sem inspeção, para facilitar a fluidez do comércio económico e evitar atrasos dos navios. Só quando o navio estava ancorado ou atracado é que as autoridades portuárias, as alfândegas e os funcionários dos serviços de imigração entravam a bordo para libertar o navio, a tripulação e a carga. Este facto tornava o porto muito vulnerável a ser alvo de organizações criminosas e terroristas. Um ataque terrorista a um porto pode afetar gravemente as populações locais, as infra-estruturas portuárias e as economias regionais dependentes das actividades portuárias.

Os regulamentos e protocolos de gestão da segurança portuária também ajudam a prevenir acidentes e, consequentemente, a reduzir a gravidade dos ferimentos em caso de acidente. É essencial porque cria um ambiente de trabalho sem perigos e com riscos mínimos. Isto melhora a qualidade das operações do terminal e a reputação do porto e pode ser considerado um instrumento comercial para atrair mais navios.

A OMI foi escolhida como a organização mais lógica para elaborar um novo código de segurança, que entrou em vigor em 1 de julho de 2004, o Código ISPS. Inicialmente centrado

na gestão da proteção física (segurança), este código destaca agora cada vez mais os riscos de cibersegurança e, no futuro, centrar-se-á também nos riscos aéreos (i.e., ataques de drones).

Nalguns portos marítimos, contudo, ainda se verificam problemas de segurança, permitindo que ameaças à segurança entrem no porto e nas suas instalações. Esta situação deve-se, em parte, ao facto de o Código ISPS nacional em vigor abordar as medidas de segurança a tomar nas instalações portuárias e não, propriamente, na zona portuária em torno desses terminais ou nas instalações/parceiros comerciais da cadeia de abastecimento dos portos.

Um porto marítimo é uma plataforma logística e industrial marítima na cadeia de abastecimento económico mundial. As actividades portuárias, como a armazenagem e a movimentação de navios, estão direta ou indiretamente ligadas a processos de transporte internacional e de informação que envolvem muitos intervenientes. Isto significa que muitas pessoas entram e saem dos acessos aos portos através de navios, camiões, caminhos-de-ferro, veículos ou como peões. O Código de Conduta e o Código ISPS exigem que todos estes movimentos sejam controlados para evitar actos ilícitos. O objetivo desta secção não é explicar a totalidade do Código ISPS ou todos os pormenores do Código de Práticas para a Segurança nos Portos, mas sim compreender como estes códigos podem ser aplicados nos portos para melhor resistir aos ataques. Todas as medidas de segurança e práticas operacionais quotidianas a seguir indicadas são descritas mais pormenorizadamente nas disposições especiais de segurança e no plano de segurança portuária.

6.4.1.1. Limites do porto e da instalação portuária

Ambos os códigos exigem que todas as pessoas sejam controladas quando entram e saem do porto ou de uma instalação portuária. Mas quais são os limites administrativos da instalação e, mais importante ainda, do porto a controlar?

As observações mostram que, nalguns portos, os capitães dos portos não sabem se são eles a pessoa a responsabilizar e o responsável final, enquanto autoridade portuária, por incidentes ocorridos a 90 milhas do mar, na baía do porto ou numa praia próxima, fora da zona visual do porto. Observámos uma confusão entre a autoridade portuária e os operadores de terminais privados para determinar quem é responsável pelos incidentes ocorridos dentro da água do cais em frente da respectiva instalação portuária. É importante incluir os limites administrativos exactos do porto e de cada instalação portuária (incluindo os limites da água) no Plano de Segurança do Porto (PSP) e no Plano de Segurança das Instalações Portuárias (PFSP). Isto permite tomar as medidas mais eficazes e contactar as pessoas certas em caso de emergência. As acções eficazes evitam os danos consequentes e asseguram o rápido restabelecimento das condições económicas normais.

6.4.1.2. Responsabilização pela segurança

As instalações portuárias são as principais responsáveis pela gestão dos incidentes de proteção ISPS. Isto significa que o oficial de proteção da instalação portuária (PFSO) deve agir em conformidade com o regulamento ISPS e o oficial de proteção do porto (PSO) deve agir em conformidade com as orientações do COP. Não compete ao PSO assumir a

responsabilidade global pelos riscos que ocorrem nas instalações portuárias, mas sim cooperar com o PFSO nesse caso.

A experiência mostra que, em alguns países, o Código ISPS foi transposto para uma lei nacional de proteção que designa o ASIP como responsável último pelos incidentes de proteção. Este facto coloca o ASIP numa situação em que o porto (e não a instalação portuária) passa a ser a parte responsável final pelos incidentes de segurança ISPS nas instalações portuárias. O resultado é que os riscos de segurança ficam por resolver porque é pouco provável que o porto invista em medidas de segurança numa concessão de instalação portuária privada.

6.4.1.3. Sistema de Gestão de Segurança (SEMS)

Para demonstrarem uma governação adequada, os departamentos de segurança portuária devem estar bem organizados e ter em conta tanto as ameaças físicas como as ciberameaças. Devem ser capazes de monitorizar e corrigir as actividades diárias de segurança e necessitam de ferramentas de gestão para o fazer. Com um sistema de gestão, podem monitorizar o estado da infraestrutura de segurança e o desempenho do pessoal de segurança e verificar se todas as funções de segurança estão a ser corretamente desempenhadas.

Em muitos portos, não existe um SEMS. Os agentes de segurança actuam por vezes como gestores de crises e concentram-se em atenuar os incidentes em vez de os prevenir. Devem gerir todos os aspectos da segurança e tomar medidas diárias para prevenir incidentes físicos, cibernéticos e híbridos. O Sistema de Gestão da Segurança da Informação (SGSI), que faz parte do SEMS, é implementado através do cumprimento dos requisitos da norma ISO 27001[55]. Todas as IC do porto devem cumprir os requisitos da norma ISO 27001 e gerir os riscos cibernéticos.

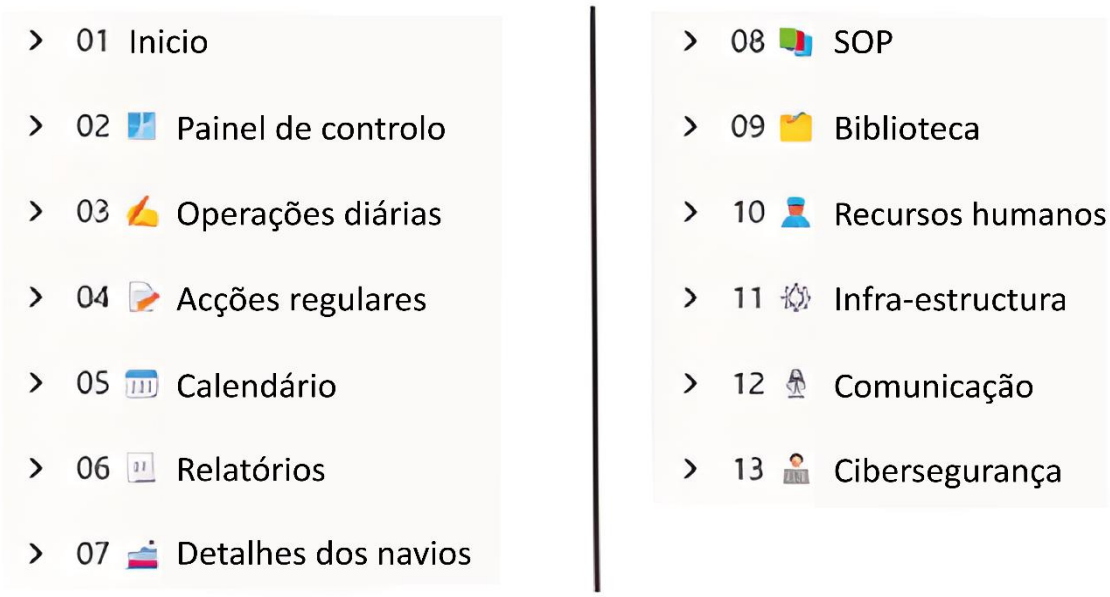


Imagem: Exemplo de um SeMS (Christophe Van Maele)

[55] (ISO/IEC 27001 e normas conexas: Gestão da segurança da informação, s.d.)

6.4.1.4. Actividades de controlo da segurança física nos portões

Cada vez que uma pessoa (a pé ou num veículo) entra nas instalações ISPS, o seu cartão de identificação (ou crachá) deve ser verificado antes de ser admitido na zona. O código exige um registo da pessoa e da hora de entrada. Quando a pessoa sai da instalação ISPS, deve ser registada a hora de saída. Isto permite saber quem se encontra na zona ISPS em qualquer altura e pode ajudar na procura de uma pessoa específica ou durante uma evacuação de emergência. A tecnologia pode ser uma grande ajuda, uma vez que as barreiras electrónicas, os torniquetes e os sistemas de cartões digitais eliminam os registos manuais propensos a erros, especialmente se uma instalação tiver várias entradas e saídas.

A realidade mostra que o registo manual continua a ser a norma em muitos portos. Além disso, as barreiras accionadas manualmente permitem o acesso do guarda, que pode decidir sem qualquer revisão da sua decisão.

Se o porto for o primeiro ponto de entrada, o que acontece frequentemente quando a zona portuária é uma zona de comércio livre, devem ser aplicados os mesmos princípios de controlo da segurança. Mais uma vez, na prática, verificam-se muitas deficiências.

6.4.1.5. Actividades de controlo de segurança na zona portuária

Os guardas de segurança móveis efectuam patrulhas e verificam se as pessoas têm autorização para entrar na zona ISPS ou na zona portuária. Para facilitar este controlo, as pessoas que se encontrem dentro da zona devem usar crachás de identificação visíveis.
No entanto, raramente são efectuados controlos de identificação, nem todas as pessoas usam visivelmente os seus distintivos.

6.4.1.6. Controlo de segurança do perímetro

O controlo perimetral é o controlo nos limites administrativos do porto ou da instalação portuária. Na maioria dos casos existem barreiras físicas, mas na União Europeia alguns terminais não críticos, como os terminais de carga geral que manuseiam areia, não precisam de ser vedados. Podem dispor de um sistema de câmaras para monitorizar os seus limites. A monitorização do perímetro é frequentemente efectuada a partir de um Centro de Controlo de Segurança, onde os operadores analisam as imagens e decidem as medidas a tomar. Os seus colegas das equipas móveis de vigilância fazem rondas de segurança física. É uma boa prática utilizar um sistema de rondas de etiquetas para garantir que verificaram todas as áreas de pontos de etiqueta. Por vezes, as rondas de identificação não são efectuadas e os operadores poderiam receber melhor formação em muitos portos.

6.4.1.7. Comunicação entre todas as partes interessadas na segurança

Deverão ser organizadas reuniões periódicas entre os ASIP e o ASIP, a fim de se actualizarem mutuamente sobre a situação atual da segurança no porto, debaterem os riscos potenciais, tratarem os incidentes e manterem-se a par dos novos desenvolvimentos no porto. Os ASIP devem realizar o mesmo tipo de reuniões a nível nacional (Comité Nacional de Segurança Marítima) com outras partes interessadas, nomeadamente a polícia portuária, as alfândegas, a marinha, as autoridades designadas e outras. Nestas reuniões são debatidas as questões de

segurança de interesse nacional e abordadas situações agudas, como a passagem ao nível de segurança 2 ou 3.

Nalguns países, as várias partes interessadas mantêm-se no seu próprio território e não se reúnem regularmente ou não se reúnem de todo. Neste caso, um plano de ação coordenado muitas vezes não existe ou existe apenas no papel, deixando espaço para que as actividades criminosas não sejam detectadas.

6.4.1.8. Reforço das capacidades através da formação do pessoal

É vital ter pessoal de segurança bem treinado e que saiba como fazer o seu trabalho. As pessoas nos portos mudam por vezes de emprego, pelo que são necessárias sessões de formação regulares para os novos recrutas e ensaios de segurança para o pessoal de segurança. Para além da formação básica ISPS, a formação no local de trabalho é igualmente importante para compreender como manipular as aplicações da sala de controlo, frequentemente digitalizadas, e como agir em caso de emergência.

A formação é considerada necessária em todos os portos do mundo. É importante manter elevados os padrões de formação para evitar que o pessoal formado não seja capaz de responder eficazmente a incidentes.

6.4.1.9. Gestão de incidentes de segurança

Se o porto tiver aplicado princípios adequados de gestão da segurança, pode considerar-se que as instalações portuárias conformes com as normas ISPS estão protegidas contra acções ilícitas intencionais. Isto inclui os princípios preventivos acima referidos, adoptados para proteger as pessoas contra o roubo, o vandalismo, o terrorismo, os ciberataques, a violência, as drogas e outras ameaças. É importante compreender que, tanto na regulamentação como na gestão quotidiana, o ISPS e o COP se baseiam na prevenção. Isto significa que as medidas de segurança portuária são adoptadas em antecipação de potenciais ameaças, antes de estas ocorrerem. Estas medidas destinam-se a dissuadir os criminosos e a reduzir a probabilidade de ocorrência de um crime ou ato de violência. As avaliações de segurança ISPS obrigatórias (processo de avaliação da privacidade e da segurança (PSA)/avaliação da segurança das instalações portuárias (PFSA)) e os planos de segurança (PSP/PSPF) constituem a base deste estado de conformidade.

Se, no entanto, ocorrer um incidente de proteção, o papel do porto pode mudar. A passagem a um nível de proteção ISPS mais elevado é uma decisão da autoridade designada. Nesse caso, é constituída uma equipa estratégica de crise e os serviços responsáveis pela aplicação da lei são chamados a intervir para fazer face à situação aguda; assim, o porto não decide geralmente por si próprio quais as medidas de segurança proactivas imediatas a tomar. As medidas a longo prazo são propostas pelo porto (instalação), aprovadas pela autoridade designada, incluídas no plano de segurança do porto (instalação) e só depois aplicadas.

Os sistemas informáticos e os sistemas de TO estão também em constante utilização. No domínio da segurança dos portos e dos terminais conformes com o ISPS, é necessário ter em conta o seguinte

- o sistema de gestão da segurança SEMS só é eficaz se for digitalizado

- o sistema de cartões de identificação é eficaz quando se trata de um sistema digital baseado numa base de dados comum a que as autoridades policiais e aduaneiras também têm acesso

- o sistema de barreira automática só admite pessoas com direito a entrar na zona
- um sistema de monitorização do perímetro com um sistema de CCTV ou outro sistema de câmaras de elevado desempenho tomará medidas inteligentes e poderá seguir as imagens de vídeo durante longos períodos de tempo
- a utilização de computadores para comunicar entre as partes interessadas permite uma ação eficiente e em tempo real quando necessário. Os sistemas de informação continuam, no entanto, a ser o domínio do departamento de TI

Até à data, vários destes sistemas de segurança não foram instalados nos portos abrangidos pelo estudo. Por conseguinte, estes portos não podem ser alvo de ataques ciberterroristas no que respeita a estes sistemas. Este tipo de risco só ocorrerá quando os sistemas de segurança destes portos forem digitalizados.

6.4.1.10. Controlo do sistema de informação

À medida que as operações de segurança quotidianas são cada vez mais digitalizadas, há uma grande quantidade de informação que tem de ser partilhada e protegida. Esta questão é descrita em mais pormenor no capítulo sobre cibersegurança.

6.4.1.11. Gestão da segurança dos navios

O Código ISPS aplica-se às instalações portuárias e a bordo dos navios. Embora o mesmo código se aplique a ambas as áreas, há vários aspectos que se aplicam apenas a bordo de um navio. Se um terrorista ganhar o controlo de um navio, da carga, da tripulação e do sistema de informação, poderá paralisar um porto durante muito tempo. O oficial de proteção do navio (SSO) é responsável pela gestão adequada da segurança a bordo, em conformidade com o Código ISPS, para evitar ataques de piratas e sequestros de navios. É supervisionado pelo oficial de proteção da companhia (CSO). Os princípios de gestão correspondem aos do porto.

Para estar preparado para ameaças externas, a OMI tomou a iniciativa de ajudar os navios com directrizes para prevenir ataques. Um navio deve ser capaz de resistir a um ataque externo através de directrizes de proteção do navio. A aplicação destas medidas de proteção divide-se num primeiro nível de defesa, num segundo nível de proteção e num último nível.

- O primeiro nível de defesa protege o navio de ser abordado por atacantes. Inclui equipas de vigilância, holofotes, manobras do navio para longe dos atacantes, arame farpado e aspersores de água e, em alguns casos, guardas armados privados.
- O segundo nível de defesa entra em vigor quando os atacantes estão a bordo e destina-se a proteger a ponte e o acesso ao castelo. Isto pode ser feito através de fechaduras nas portas, sensores de movimento, sistemas de CCTV e uma tripulação vigilante.
- O terceiro nível de defesa é ativado se os atacantes tomarem conta da ponte e tiverem acesso ao sistema de informação. Nesse caso, a tripulação pode esconder-se num bunker construído para o efeito, denominado Citadel, onde estão disponíveis os

controlos vitais do motor e da direção e onde o sistema de comunicações pode ser monitorizado.

A tripulação deve compreender perfeitamente como tudo funciona na Cidadela e quais são os meios importantes para manter o controlo da nave a partir de lá. Se não forem

devidamente treinados para controlar a nave a partir deste espaço, a própria Cidadela pode tornar-se uma prisão fatal para a tripulação ali reunida para sua própria proteção.

6.4.2. Gestão de cibersegurança

O modelo de gestão da cibersegurança desenvolvido pela BIMCO[56] (baseado no Quadro de Gestão do Risco (RMF) do NIST)[57] segue as etapas gerais de avaliação da segurança descritas na secção 6.4 e contém os seguintes componentes relativos à gestão do risco cibernético:

1. Identificar ameaças
2. Identificar vulnerabilidades
3. Avaliar a exposição ao risco (estimativa do risco)
4. Desenvolver medidas de proteção e deteção
5. Estabelecer planos de emergência
6. Responder e recuperar de incidentes de cibersegurança

O ponto mais crucial quando se lida com a cibersegurança é identificar o cenário de ameaças, o que significa praticamente identificar quais são as possíveis ameaças que podem afetar os bens de IC marítimos. Alguns exemplos de ciberameaças que foram identificadas durante o ano de 2020 pela ENISA[58] são: (1) Malware, (2) Ataques baseados na Web (3) Phishing, (4) Ataques a aplicações Web, (5) Spam, (6) DDoS, (7) Roubo de identidade, (8) Violação de dados, (9) Ameaça interna, (10) Botnets, (11) Manipulação física, danos, roubo e perda, (12) Fuga de informação, (13) Ransomware, (14) Ciberespionagem, (15) Crypto jacking.

Logo que o cenário de ameaças seja identificado, a superfície de ataque - o conjunto de todos os ataques que podem ser utilizados para explorar as ameaças - dos bens das IC pode ser facilmente identificada (ponto 4 do ponto 6.4). A superfície de ataque destes bens pode ser determinada com base nas suas vulnerabilidades, pelo que é necessário proceder a uma avaliação das vulnerabilidades.

A etapa seguinte identificada na BIMCO consiste em avaliar a exposição ao risco relativamente aos activos de IC. Em particular, o risco é dividido em quatro tipos de resposta ao risco, ou seja, a:

- *evitar o risco*: neste caso, o risco não é aceite (deve ser tomada uma decisão pela gestão de topo do porto , mediante recomendação do CISO (Chief Information Security Officer))
- *transferir o risco* (ou seja, para uma companhia de seguros): uma decisão da direção

[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)

de topo do porto também tem de ser tomada por recomendação do CISO uma vez que pode ter impacto financeiro

- *tomar medidas de mitigação*: a mitigação do risco é também uma decisão que deve ser tomada pela gestão de topo do porto, mediante recomendação do CISO , uma vez que também pode ter impacto financeiro
- *o risco é aceite*: a aceitação do risco é uma decisão comercial direta e só a gestão de topo pode tomar esta decisão.

Para atenuar o risco, é necessário desenvolver medidas de proteção e deteção e estabelecer um plano de resposta para reduzir o risco para um nível aceitável. O nível aceitável é definido pela IC marítima (**apetência pelo risco**) após a realização de uma análise custo-benefício ou após a identificação do impacto do risco no negócio. A **matriz de apetência pelo risco** descreve uma análise qualitativa do risco:

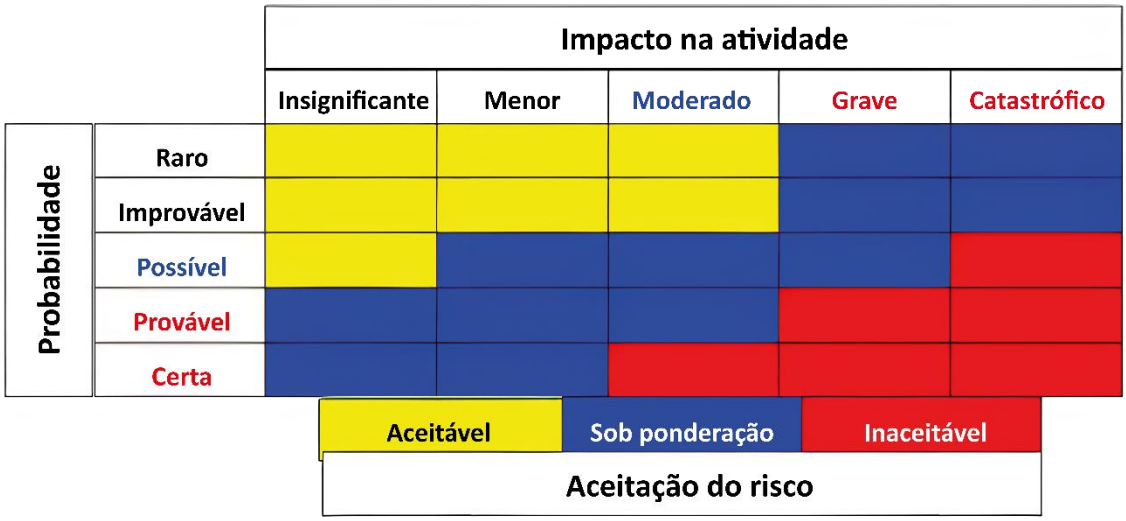


Figura 10**:** Matriz de apetência pelo risco

Se as medidas de mitigação não conseguirem fazer com que o risco atinja um nível aceitável de acordo com a matriz de apetência pelo risco, a gestão de topo do porto terá de tomar uma decisão comercial no sentido de aceitar ou não o risco.

Os riscos têm de ser avaliados caso a caso, de acordo com o ecossistema cibernético da IC e, consequentemente, têm de ser definidos como i) aceitáveis, ii) riscos a discutir (medidas de atenuação ou transferência de riscos), iii) inaceitáveis, que têm de ser evitados.

As orientações da BIMCO sobre cibersegurança a bordo dos navios baseiam-se em princípios de alto nível:

- sensibilização para os riscos de segurança, proteção e comerciais que se apresentam devido à falta de medidas de cibersegurança;
- proteção da infraestrutura informática de bordo e do equipamento ligado;
- sistema de autenticação e autorização dos utilizadores, para garantir o acesso adequado às informações necessárias;

- proteção dos dados utilizados no ambiente do navio, garantindo uma proteção adequada em função da sensibilidade da informação.

Figura 11: Abordagem de gestão da cibersegurança da BIMCO[59]

- gestão dos utilizadores de TI, para garantir que só têm acesso e direitos às informações para as quais estão autorizados;
- gestão das comunicações entre o navio e a terra, e
- desenvolvimento e aplicação de um plano de resposta a incidentes cibernéticos com base numa avaliação dos riscos.

O valor dos activos portuários (importância nas operações marítimas) determina os requisitos de segurança e os controlos a efetuar. Vários esforços (e.g., projeto SAURON) contribuem para classificar os activos portuários e propor arquitecturas de segurança.

[59] (The Guidelines on Cyber Security onboard Ships - Version 4, 2020)

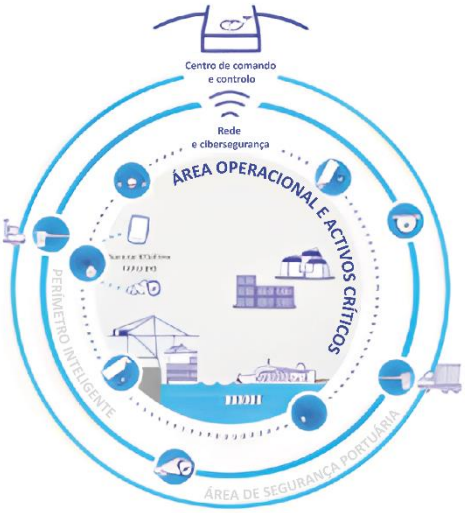


Figura 12: Arquitetura de segurança física e cibernética do SAURON[60]

Esta abordagem contribui para a segurança dos portos, garantindo a segurança dos activos físicos e a cibersegurança dos activos cibernéticos.

6.5. Ciber-resiliência marítima

Ciber-resiliência marítima[61] é a capacidade da IC marítima para resistir a ataques. A resiliência é alcançada se a segurança (segurança e cibersegurança) for garantida e se a estrutura de governação for eficaz e auditável, por exemplo, se a força dos controlos e os procedimentos de segurança (como os procedimentos de recuperação de desastres) forem regularmente testados.

Figura 13: Resiliência marítima

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

Várias organizações adoptam uma visão mais geral da segurança, por exemplo, de acordo com a Instituição de Engenharia e Tecnologia (IET)[62], a segurança procura atingir e manter oito objectivos gerais de segurança, como se mostra a seguir:

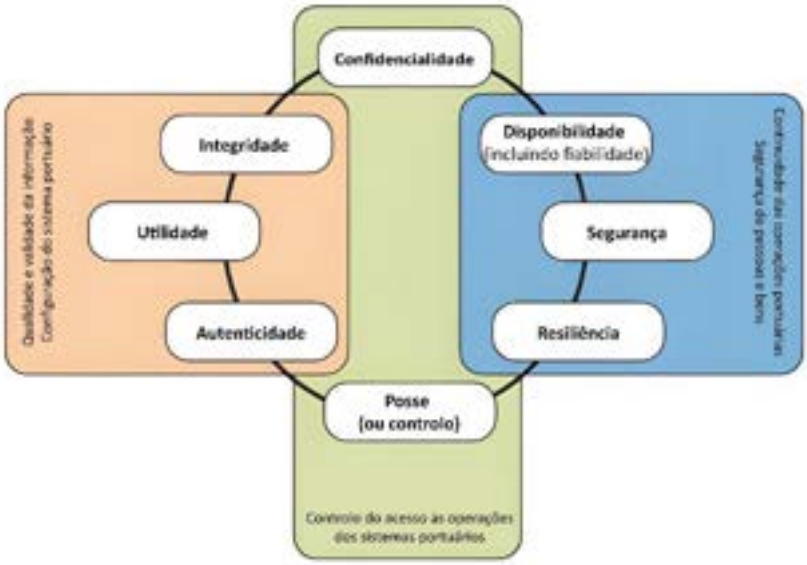


Figura 14: Objectivos de segurança das IET

6.6. Factores humanos

A natureza humana, o comportamento, os valores sociais, culturais e éticos fazem do indivíduo o principal facilitador dos ataques à cibersegurança ou um defensor competente da cibersegurança ou um operador e oficial marítimo consciente da segurança. Os perfis humanos e as suas características desempenham um papel importante nos futuros avanços na proteção dos bens e infra-estruturas marítimas.

A investigação dos factores humanos e dos parâmetros dos membros das equipas de segurança dos portos e navios ou o estudo dos perfis dos atacantes (a partir de incidentes de segurança anteriores) ajuda a prever ou prevenir um incidente e a gerir mais eficazmente um ataque.

Além disso, ao identificar os perfis do pessoal marítimo (por exemplo, operadores, agentes, administradores, membros da tripulação), a IC marítima pode desenvolver uma formação em matéria de segurança mais eficaz que responda às suas necessidades e aos seus níveis de compreensão da segurança. Os planos e procedimentos de segurança têm de ser claros para todos os funcionários, de modo a que estes os utilizem e adoptem[63] diariamente. O desenvolvimento de procedimentos de segurança aplicáveis requer o envolvimento dos trabalhadores no desenvolvimento desses procedimentos.

[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)

O fator humano é o ponto de viragem na segurança global do ecossistema marítimo. Normalmente, os portos e os navios são os elos mais fracos da cadeia de segurança, comprometendo as operações e os serviços marítimos apesar dos meios tecnológicos existentes; as pessoas são a maior ameaça.

A sensibilização das partes interessadas do sector marítimo para a segurança deve ser objeto de um acompanhamento contínuo; a distribuição e a análise dos questionários constantes do anexo podem contribuir para esse fim. As campanhas de sensibilização e a formação prática orientada são os meios para preparar os trabalhadores marítimos e as partes interessadas para se tornarem os principais guardas de segurança e defensores dos ataques físicos e cibernéticos no ecossistema marítimo e para reforçar a cultura marítima de segurança.

7. Práticas de segurança dos portos em África

7.1. Os portos do Golfo da Guiné

Cerca de 1500 navios por dia (petroleiros, cargueiros e navios de pesca) navegam nas águas do Golfo da Guiné dirigindo-se a 20 portos importantes. Este importante fluxo económico cria uma oportunidade de ouro para a pirataria e o rapto de marítimos, os assaltos à mão armada no mar, a pesca ilegal, o contrabando e o tráfico de seres humanos nos portos e nas suas imediações, bem como para a criminalidade organizada transnacional e os atentados terroristas. Representa uma grande ameaça para a segurança marítima de todos os navios que frequentam estes portos e, em última análise, para o desenvolvimento económico dos países de toda a região.

Prevê-se que o potencial económico da região do Golfo da Guiné aumente ainda mais nos próximos anos, mas antes de poder concretizar e beneficiar deste potencial, é necessário enfrentar primeiro as ameaças à sua estabilidade e prosperidade. Para o efeito, é necessário identificar e abordar continuamente os desafios de segurança relacionados com o mar, os portos marítimos e o interior.

Figura 15: Região marítima do Golfo da Guiné[64]

7.2. Organização da segurança portuária em África

Os portos marítimos em África estão organizados da mesma forma que outros portos em todo o mundo. A autoridade portuária é gerida, nas suas operações quotidianas, por funcionários do Estado, que são responsáveis perante os respectivos ministérios.

Uma autoridade portuária tem vários departamentos. Um deles é o departamento de TI e o outro é o departamento de operações, que é chefiado pelo capitão do porto. As observações

[64] (Mapa do Golfo da Guiné, 2021)

efectuadas em portos de todo o mundo mostraram que o capitão do porto é nomeado como o responsável geral, para além das operações náuticas, pela segurança no porto e nas instalações exploradas pelo próprio porto. O departamento de segurança deve aplicar a regulamentação ISPS no porto e fazer cumprir o escudo de proteção. O departamento de segurança do porto, por outro lado, concentra-se na segurança humana e mantém quase sempre uma equipa de intervenção que actua em caso de incêndio e primeiros socorros. A nível administrativo, o departamento de TI do porto fornece regras de cibersegurança relacionadas com os sistemas administrativos gerais do porto, mas a infraestrutura de segurança ISPS está muitas vezes fora do seu âmbito e é efectuada pelas empresas externas que instalaram o hardware de segurança. Os portos recebem receitas baseadas no volume de carga dos navios dos seus clientes através da "sobretaxa ISPS". Esta taxa cobre o custo do conjunto global de medidas destinadas a melhorar a proteção ISPS das instalações portuárias.

Um exemplo de uma boa prática de segurança inclui a seguinte arquitetura de TI:

Existem 4 sistemas principais de segurança de TO e TI que são cruciais para evitar um incidente de segurança. Se algum destes sistemas for atacado por um ciberataque, a integridade da segurança física do porto fica comprometida.

- O primeiro sistema é o *sistema de cartões de TO*: O sistema de crachás baseia-se numa base de dados digital das pessoas que fazem negócios no porto. A base de dados é constituída por pessoal do porto, trabalhadores portuários, camionistas, clientes e visitantes. Depois de um controlo administrativo inicial (pela polícia) quando se solicita um crachá, a pessoa é autorizada a entrar no porto em determinados dias e a determinadas horas. Na melhor das hipóteses, a base de dados é verificada regularmente pela polícia, que pode bloquear pessoas com intenções nefastas. Um sistema de cartões será instalado por uma empresa de segurança externa, que terá direitos de administração para manter o sistema de TO. O pessoal de segurança do porto produz e distribui os crachás. Se o sistema de crachás for pirateado e o tempo de acesso for alargado, um criminoso pode receber um crachá do porto e entrar na zona portuária sem ser detectado.
- O segundo sistema de segurança é o *sistema de controlo do acesso ao porto*: Este sistema permite que as pessoas entrem nas instalações do porto (e das instalações portuárias) quando mostram o seu cartão dentro do período de tempo autorizado. O sistema de controlo de acesso acede à base de dados dos cartões e decide se abre portões, portas, torniquetes, barreiras de acesso, etc. O sistema de controlo de acesso é normalmente instalado pelo mesmo integrador de segurança que o sistema de cartões. Se o sistema de controlo de acesso puder ser induzido em erro por um ciberataque, os criminosos (e o seu contrabando) têm livre acesso à entrada e saída do porto.
- O terceiro sistema é o *sistema de controlo do perímetro Tecnologia Operacional (TO)*: Para controlar o perímetro do porto, são necessárias vedações e um sistema de monitorização para controlar a entrada ilegal. Atualmente, os sistemas de CCTV, bem como os sistemas de câmaras térmicas e de infravermelhos, são utilizados nos portos civis e nas instalações portuárias para verificar a integridade da vedação. Além disso, é construída uma sala de controlo de segurança para monitorizar e atuar em caso de intrusão e violação. Estes sistemas de câmaras são instalados por empresas externas

especializadas que têm direitos administrativos sobre o sistema. As câmaras são operadas pelo pessoal de segurança do porto. Se o sistema de câmaras fosse pirateado por um ciberataque, os guardas poderiam ser induzidos em erro e ver imagens falsas, permitindo a entrada ilegal ou o roubo através das vedações do perímetro.

Figura 16: Sistema de controlo de perímetro de TO[65]

- O quarto sistema é o *sistema informático*: O sistema informático utilizado pelo pessoal de segurança é constituído principalmente por um sistema de gestão da segurança SeMS, documentos de escritório digitais, correio eletrónico e ligação à Internet. Este sistema é instalado pelo serviço informático do porto, que mantém o controlo administrativo do escudo de cibersegurança. Se os operadores forem aliciados para um ciberataque, utilizando, por exemplo, uma pen USB infetada, a comunicação entre os guardas de segurança pode ser impedida, dando origem a uma situação de segurança cega.

Noutros portos da África do Sul e Oriental, são aplicados os mesmos princípios de segurança que nos portos do Golfo da Guiné. Os operadores portuários privados que detêm instalações portuárias concessionadas organizam-se de modo a garantir a segurança e a conformidade com as normas ISPS.

As autoridades portuárias concentram-se em manter a zona portuária comum segura e protegida dentro dos limites do porto administrativo. Tomam medidas para proteger esta zona, desde a zona de ancoragem, as zonas de amarração, até às docas do porto e toda a zona portuária (zonas privadas exclusivas).

7.3. Iniciativas internacionais para os portos africanos

Existem vários projectos centrados principalmente na melhoria da segurança em alto mar, na pirataria, nas acções transfronteiriças e na droga:

[65] Foto tirada por Christophe Van Maele

- Os EUA estão presentes com o seu programa do Comando Africano dos EUA (AFRICOM), centrado em iniciativas de segurança no alto mar por navios de guerra e apoio às marinhas locais.
- Os países do Golfo da Guiné e das suas imediações assinaram o "Código de Conduta relativo à Repressão da Pirataria, dos Assaltos à Mão Armada contra Navios e das Actividades Marítimas Ilícitas na África Ocidental e Central" (Código de Conduta de Yaoundé). Esta arquitetura de Yaoundé promove a cooperação marítima regional e salvaguarda um ambiente marítimo estável.
- A Europa está presente com o programa Rotas Marítimas Críticas (CMR). Um conjunto de projectos centrados no quadro jurídico, nas regras operacionais, na partilha de informações, na formação e no reforço das capacidades.
- A rede inter-regional do Golfo da Guiné (GoGIN) tem por objetivo reforçar o conhecimento do domínio marítimo da rede de partilha de informações regionais da arquitetura de Yaoundé (YARIS).
- O apoio à Segurança Marítima Integrada da África Ocidental (SWAIMS) visa melhorar os quadros de aplicação da lei e de governação.
- O Programa de Apoio à Estratégia de Segurança Marítima na África Central (PASSMAR) centra-se na cooperação marítima transfronteiriça.
- O Projeto de Cooperação nos Portos Marítimos (SEACOP) visa desenvolver capacidades e reforçar a cooperação contra o tráfico ilícito marítimo.
- Organizações internacionais como a Interpol e o Programa de Interrupção Global de Redes Criminosas (CRIMJUST) do UNODC estão a concentrar-se nas rotas do tráfico de droga.

A decisão de como lidar com a segurança e a cibersegurança nos portos é da exclusiva responsabilidade do país e o envolvimento internacional tem de ser aprovado a nível nacional.

- Projeto de Segurança Portuária da África Ocidental e Central (WeCAPS),[66] um projeto da CMR na região do Golfo da Guiné) visa melhorar a segurança portuária e cumprir o ISPS. Este projeto analisa os riscos em 10 portos da região do Golfo da Guiné e executa acções de segurança relativas à formação de pessoal, aconselhamento especializado e implementação do SeMS.
- A IMO[67] e a Guarda Costeira dos Estados Unidos (USCG)[68] desempenham um papel importante nos portos marítimos vinculados ao ISPS e estão presentes com várias actividades de formação, visitas de melhoria e projectos de assistência nos portos africanos.

7.4. Riscos cibernéticos em África

Com a crescente digitalização do sector marítimo e o aumento do poder das ferramentas à disposição dos cibercriminosos, o número de ciberataques aumentou, incluindo ataques a navios e a portos marítimos que se aproximam. Embora a maior parte dos incidentes de cibersegurança marítima até à data não tenha visado os portos africanos, os dados

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

disponíveis sobre ciberataques noutros sectores e portos noutras partes do mundo ajudam a fornecer informações valiosas aos governos africanos e às autoridades portuárias.

Estes ciberataques representariam uma ameaça existencial para a economia do continente africano se os portos fossem atacados. Um relatório recente do Instituto de Estudos de Segurança [69] sobre a cibersegurança africana no mundo marítimo mostra como a cibersegurança se está a tornar rapidamente um aspeto importante das necessidades africanas em matéria de segurança marítima, à medida que a digitalização se instala na indústria marítima africana. Com as actuais mudanças tecnológicas nos navios, os portos africanos terão de aumentar o seu escudo de cibersegurança para se manterem competitivos. Os portos africanos precisam de pensar de forma diferente sobre as ameaças, os riscos e as vulnerabilidades, bem como sobre as acções criminosas.

Os navios estão a liderar a abordagem das medidas de cibersegurança e são obrigados a incluir medidas de cibersegurança no seu manual ISM e são desafiados pela OMI e pelas suas companhias de seguros a levar a cibersegurança a sério. Em contraste com as iniciativas a bordo dos navios, os portos marítimos da África Subsariana continuam a enfrentar desafios em matéria de segurança e cibersegurança para melhorar o seu escudo.

Um ciberataque digno de nota teve lugar em julho de 2021, quando a Transnet, uma importante empresa portuária sul-africana, que gere 60% do tráfego de contentores do país no porto de Durban (África do Sul), foi atingida por um ataque de ransomware. Este ataque causou enormes perturbações. Os seus terminais de contentores em Durban, Ngqura, Port Elizabeth e Cidade do Cabo tiveram de passar ao processamento manual da carga até que os sistemas informáticos fossem restabelecidos. O resultado foi um enorme congestionamento de mais de 14 horas para os camiões recolherem e descarregarem contentores e a inevitável perda de receitas para o operador do terminal. A ISS previu no mesmo relatório que incidentes como o ataque à Transnet irão aumentar em toda a África Subsariana, uma vez que os portos marítimos são alvos atractivos, ainda vulneráveis a ciberataques. Neste caso, a infraestrutura de transportes, especialmente um porto, é um alvo lucrativo para os cibercriminosos ou outros agentes hostis devido à escala das operações e ao elevado impacto mediático internacional.

Embora os principais portos da África Subsariana disponham de departamentos de sistemas de TI, a implementação e o cumprimento de medidas concretas de cibersegurança estão longe de ser alcançados, e esta situação representa um risco claro para a segurança. Os responsáveis políticos dos portos compreendem que é necessário fazer progressos e demonstram grande interesse em melhorar o escudo de cibersegurança nas suas operações e sistemas de segurança, como os sistemas de CCTV, os sistemas de cartões e os sistemas de controlo de acesso. No entanto, as mesmas autoridades portuárias não dispõem de conhecimentos suficientes para melhorar a sua ciber-resiliência e parece haver poucas campanhas de sensibilização conduzidas pelos decisores políticos nacionais junto dos portos

[69] (Reva, 2020)

para reduzir os riscos cibernéticos. Não existem muitos protocolos cibernéticos nos departamentos de segurança portuária.[70]

Um dos projectos da CE no Golfo da Guiné (WeCAPS) tomou a iniciativa de garantir que o pessoal portuário, a diferentes níveis, esteja consciente das ciberameaças e dos riscos associados e seja capaz de agir em conformidade. O projeto centra-se na formação de sensibilização dos operadores e do pessoal e, se o tempo do projeto o permitisse, teria realizado mais acções de melhoria a nível das infra-estruturas (sistemas de acesso, sistemas de cartões, sistemas CCTV e sistemas de comunicação). O apoio deste projeto é coerente com as melhores práticas destacadas por outras iniciativas, nomeadamente a publicação das Orientações de Cibersegurança para Portos e Instalações Portuárias do IAPH 2021 e as Orientações de Gestão do Ciber-Risco Marítimo da IMO.

Para além da abordagem ascendente da WeCAPS, uma lei nacional sobre ciber-resiliência seria bem acolhida pelos decisores portuários. A União Africana deu um passo positivo em 2014 com a adoção da Convenção sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo) [71] e poderia ser o primeiro passo para esta legislação. Além disso, os países africanos e os operadores de terminais privados poderiam adotar conjuntamente as melhores práticas para garantir a segurança das suas infra-estruturas marítimas.

[70] (Africa's Maritime Cyber Security Progress After the Transnet Attack, 2021)
[71] (African Union Convention on Cyber Security and Personal Data Protection, 2014)

8. Conclusões

As ICI marítimas incluem, entre outros, portos, navios e companhias marítimas. As ICI marítimas são seguras se os seus activos físicos forem seguros e os seus activos cibernéticos forem ciberseguros. Este estudo abrangeu todos os aspectos importantes para a segurança das ICI marítimas, incluindo: jurídicos e políticos, tecnológicos, normas e directrizes.

9. Recomendações

O objetivo do presente estudo não é criar um manual de boas práticas, mas sim enumerar sucintamente as questões que devem ser abordadas para construir um escudo cibernético de elevado desempenho. As melhores práticas a seguir referidas ajudarão os operadores portuários e de navios a cumprir os requisitos de gestão dos riscos de cibersegurança da IMO, reforçando a segurança e a fiabilidade das cadeias de abastecimento e do comércio internacionais.

9.1. Recomendações para os portos da África Subsariana

Tal como demonstrado no presente relatório, é essencial adotar uma abordagem holística da segurança. Estas primeiras recomendações incidem na segurança física, que complementaria as recomendações para melhorar a cibersegurança enumeradas mais adiante. As recomendações baseiam-se em observações efectuadas em vários portos da África Subsariana, onde é possível melhorar o escudo de segurança:

1. Apoio internacional aos países africanos para optimizarem a sua legislação nacional de proteção do transporte marítimo aplicável às zonas portuárias administrativas jurídicas, através da avaliação da atual regulamentação da polícia portuária e das alfândegas, da regulamentação nacional ISPS e de segurança portuária e de outras regulamentações nacionais.
2. Reforçar a capacidade do pessoal de segurança através de várias iniciativas, tais como:
    - Formação de pilotos de drones (contra potenciais ataques aéreos)
    - ISPS Formação de agentes de segurança de instalações portuárias e formação de guardas de segurança em cooperação com a OMI
    - Guardas de segurança com cães de segurança treinados (contra drogas, produtos químicos, explosivos)
    - Formação de gestão do pessoal de segurança em sistemas de gestão da segurança SEMS
    - Aconselhamento especializado sobre a instalação de sistemas de controlo de acesso, sistemas de controlo perimetral e centros de controlo de segurança portuária
    - Formação da tripulação de embarcações RIB e formação em interceção nas zonas portuárias
    - Formação em vigilância para as tripulações de embarcações, a fim de evitar ataques de piratas a navios fundeados
    - Formação da polícia portuária sobre as tarefas de segurança portuária e a regulamentação ISPS
    - Formações em matéria de inspeção e auditoria para as autoridades designadas e a inspeção pelo Estado do porto
    - Instalação de comités de segurança portuária com a participação de actores privados e governamentais

3. Fornecer equipamento crítico para o pessoal de segurança nos portos e para os operadores de terminais privados, permitindo-lhes executar as suas tarefas de forma eficiente, tais como
    - Drones para a polícia e o pessoal de segurança
    - Barcos insufláveis rígidos (RIB) para guardas de segurança de patrulha marítima e polícia
    - Equipamento de comunicação para o pessoal de segurança em terra e na água
    - Equipamento de inspeção para guardas de segurança nas entradas dos portos
    - Sistemas de marcação para guardas de patrulha móveis
    - Scanners de raios X para inspecionar a carga para a alfândega
4. Acompanhar a marinha, a polícia e as autoridades portuárias e marítimas designadas nos seus esforços para melhorar os procedimentos operacionais normalizados e o planeamento da resposta a emergências nas zonas portuárias ligadas à água, a fim de reforçar a segurança dos navios ancorados, dos canais de acesso aos portos e das bacias portuárias.
5. Reforçar a relação entre os diferentes intervenientes portuários nos vários países através de seminários de partilha de conhecimentos e workshops técnicos. Envolvendo os Ministérios dos Transportes e da Segurança Nacional, Autoridades Designadas, decisores portuários, portos da Europa e de outros países, IMO, USCG, Comissão Europeia, The Shipowners' Club - Protection and Indemnity (P&I) e outras organizações seguradoras, companhias de navegação e operadores de terminais privados activos no continente.

9.2. Recomendações aos intervenientes marítimos africanos

Os países africanos em geral precisam de melhorar a sua legislação em matéria de cibersegurança, à semelhança de muitos outros países do mundo com fronteiras marítimas. Para além das iniciativas de segurança portuária, constata-se que vários portos ainda enfrentam desafios para tornar os seus portos altamente resistentes a ataques de segurança e cibersegurança. Por conseguinte, são necessárias iniciativas adicionais em matéria de segurança portuária, com o apoio dos legisladores nacionais, das autoridades portuárias, dos operadores de terminais privados, das autoridades nacionais designadas, da polícia, das empresas privadas de segurança portuária e de outras partes interessadas nos portos e nas suas imediações. Recomenda-se vivamente que estas iniciativas ISPS sejam reforçadas juntamente com iniciativas de cibersegurança na zona jurídico-administrativa do porto (em terra e na água). Estas iniciativas criariam um quadro operacional através do reforço das capacidades, do apoio ao desenvolvimento de infra-estruturas e equipamentos adequados, da formação e treino e do alargamento das parcerias internacionais.

9.3. Apoio à gestão de topo

Os quadros superiores estão cada vez mais conscientes das ameaças e riscos cibernéticos e do seu impacto potencialmente devastador nas operações dos navios e dos portos. O investimento contínuo necessário em cibersegurança visará especificamente o pessoal de cibersegurança, a gestão da segurança, os processos e as tecnologias. Para tal, é necessário afetar orçamento e recursos, que devem ser aprovados e apoiados pelos quadros superiores. Os riscos cibernéticos afectam, e podem ser afectados por, todas as pessoas nos portos e nos navios. Por conseguinte, as medidas de cibersegurança não devem ser da responsabilidade exclusiva do departamento de TI.

9.4. Formação de sensibilização para a cibersegurança

Todas as pessoas a bordo de um navio ou num porto devem estar cientes das ameaças e da forma como os ciberincidentes as afectam. Por conseguinte, devem receber formação de sensibilização para o ciberespaço, de modo a saberem o que podem fazer para garantir a segurança do porto e do navio. A formação deve ser adaptada a cada função.

9.5. Procedimentos, directrizes e instruções de cibersegurança

O pessoal dos portos e dos navios tem de saber exatamente o que se espera deles e como gerir a cibersegurança. Devem receber Procedimentos Operacionais Normalizados (SOP) sobre a forma de gerir as suas tarefas diárias e a gestão de incidentes. Devem ser formadas equipas de cibersegurança, que se reúnam regularmente e tenham impacto nas operações.

9.6. Serviços e funções críticos na organização

Para saber como lidar com a cibersegurança, é vital saber quais os sistemas existentes no porto e a bordo dos navios. Um inventário deve incluir todos os activos físicos e cibernéticos críticos, incluindo dispositivos, sistemas, software e aplicações para TI e TO.

9.7. Avaliação dos riscos de cibersegurança

Com o inventário em mãos, deve ser efectuada uma avaliação dos riscos para identificar ameaças, riscos e vulnerabilidades relacionados com os activos de TI e TO que possam ter um impacto negativo nas operações e na segurança.

9.8. Plano de gestão da cibersegurança

Para além dos planos de segurança ISPS do porto (instalações) e dos planos de segurança dos navios, deverá ser elaborado um plano de gestão da cibersegurança, uma vez que estes planos se centram principalmente na segurança física. Este plano incluirá medidas para fazer face aos riscos identificados com base na avaliação de riscos, as responsabilidades da tripulação em matéria de cibersegurança, os procedimentos de resposta às ameaças à cibersegurança e os procedimentos de auditoria das actividades de cibersegurança. O plano deve incluir medidas processuais e técnicas a aplicar para minimizar os riscos cibernéticos.

9.9. Cibersegurança da cadeia de abastecimento

Os fornecedores de equipamento podem ter acesso remoto a sistemas críticos a bordo (e.g. sistemas de navegação, sistemas de alimentação de motores, sistemas de carga, etc.) ou nas instalações portuárias (e.g. espalhadores de contentores, gruas portuárias, sistemas RMG e RTG, etc.), e qualquer incidente de cibersegurança do lado do fornecedor pode afetar o navio ou os equipamentos e sistemas de movimentação específicos pelos quais é responsável. Por conseguinte, é importante avaliar a cibersegurança dos fornecedores para identificar riscos nos seus serviços e sistemas que possam afetar negativamente o funcionamento dos navios e dos portos.

9.10. Gestão, resposta e recuperação de incidentes

Os navios e portos devem aplicar políticas, procedimentos e controlos adequados que lhes permitam detetar, responder, recuperar e aprender os incidentes de cibersegurança.

9.11. Normas e quadros de cibersegurança

Não é fácil gerir todos os aspectos da gestão da cibersegurança sem recorrer à ajuda e orientação das normas e directrizes existentes. Por conseguinte, a gestão da cibersegurança deve utilizar políticas, processos e procedimentos de controlo técnico e de sensibilização dos trabalhadores para gerir a cibersegurança nos portos e a bordo dos navios. O aconselhamento especializado de consultores marítimos que possam ajudar a implementar a cibersegurança no ambiente do porto e do navio é importante para evitar erros.

9.12. Recomendações gerais sobre a cibersegurança do porto

As recomendações de cibersegurança a seguir enumeradas, a aplicar nos portos marítimos, farão uma diferença positiva em termos de cibersegurança para as autoridades portuárias e outras partes interessadas que trabalham no porto.

1. Legislação do porto sobre cibersegurança

Implementar/ajustar a legislação nacional de modo a torná-la conforme com a legislação, os códigos e as directrizes internacionais em matéria de cibersegurança portuária, uma vez que esta é o motor de um comércio internacional fiável.

2. Avaliação da cibersegurança (CSA)

De acordo com as normas de segurança ISPS, são efectuadas avaliações da segurança (PSA e PFSA) dos portos e instalações portuárias. O objetivo destas avaliações é identificar as vulnerabilidades das estruturas físicas, dos sistemas de proteção do pessoal e dos processos empresariais susceptíveis de conduzir a um incidente de segurança. A avaliação da cibersegurança deve basear-se nas avaliações de segurança ISPS existentes, se for caso disso. Utilizar as normas existentes (e.g., ISO270xx) e as melhores práticas internacionais (e.g., IMO/BIMCO, ENISA, IACS) para avaliar, estimar e atenuar os riscos cibernéticos e físicos.

3. Plano de cibersegurança (CSP)

As avaliações de proteção constituem a base dos planos de proteção do porto (PSP) e da instalação portuária (PFSP). Estes planos abordam as questões identificadas na avaliação pertinente, estabelecendo medidas de proteção adequadas destinadas a minimizar a probabilidade de violação da proteção e as consequências dos riscos potenciais. O plano de cibersegurança deve basear-se no PSP ou PFSP existente, se for caso disso. Testar um plano, de preferência com exercícios de mesa, também é importante para garantir que o plano está atualizado e é compreendido por todas as partes interessadas.

O PEC tem a mesma função que o plano de proteção ISPS no que se refere às questões identificadas na avaliação da segurança, tendo igualmente em conta o impacto das medidas estabelecidas nas disposições especiais de segurança e no plano de proteção da segurança.

4. Organização cibernética

Para a gestão da cibersegurança, é fundamental dispor de um organigrama que atribua funções e tarefas específicas às diferentes partes interessadas.

- A nomeação de um oficial de cibersegurança do navio (CYSO), responsável pela cibersegurança do porto e das instalações portuárias geridas pelo porto.

- Instalação de um Comité de Segurança Portuária, com a participação de diferentes partes interessadas.
- A criação de um Centro de Operações de Segurança (SOC).

5. Gerir a cibersegurança

Após a criação do escudo de cibersegurança através do estabelecimento da CSA e do CSP, é importante que o SOC disponha de disposições operacionais e de gestão adequadas, incluindo:

- Auditoria e revisão regulares do PEC
- Testes regulares de ciberataques
- Acompanhamento da evolução do escudo cibernético
- Métodos para fornecer informações a terceiros
- Como gerir os incidentes de segurança
- Testes regulares dos planos e da gestão de incidentes através de exercícios de mesa

6. Formação para o reforço das capacidades

As pessoas trabalham com sistemas informáticos e de TO e necessitam de formação regular para trabalharem de forma eficiente. Por conseguinte, a formação a diferentes níveis é vital:

- Formação do pessoal de segurança (operadores), que utiliza diariamente os sistemas informáticos e os de TO de segurança.
- Formação para a gestão da segurança (PFSO, PSO), para compreender as consequências e o impacto na segurança dos sistemas informáticos e de TO. Devem ser capazes de minimizar os danos, aplicar contramedidas de segurança imediatas e regressar à situação normal o mais rapidamente possível.
- Formação do pessoal informático que participa na segurança dos sistemas informáticos. Devem ser capazes de instalar e melhorar o escudo de cibersegurança para o pessoal de segurança.

As recomendações de segurança acima referidas são descritas no quadro seguinte:

N°	Recomendações
1	Otimizar a legislação nacional em matéria de proteção do transporte marítimo (regulamentos da polícia portuária e das alfândegas, regulamentos nacionais ISPS e de segurança portuária)
2	ISPS Formação de agentes de segurança de instalações portuárias e formação de guardas de segurança em cooperação com a OMI
3	Guardas de segurança com cães/formação em portões inteligentes (contra drogas, produtos químicos, etc.)
4	Formação do pessoal de segurança em sistemas de gestão da segurança SEMS
5	Aconselhamento sobre a instalação de sistemas de controlo de acesso, sistemas de controlo perimetral e centros de controlo de segurança portuária
6	Formação da tripulação de embarcações RIB e formação em interceção nas zonas portuárias
7	Formação em vigilância para as tripulações de embarcações, a fim de evitar ataques de piratas a navios fundeados

8	Formação da polícia portuária sobre as tarefas de segurança portuária e a regulamentação ISPS
9	Formação em matéria de inspeção e auditoria para as autoridades designadas e a inspeção pelo Estado do porto
10	Instalação de comités de segurança portuária com a participação de actores privados e governamentais
11	Fornecer equipamento de segurança certificado para o pessoal de segurança nos portos e para os operadores de terminais privados (drones, RIBS, equipamento de comunicação, equipamento de inspeção, sistemas de marcação e scanners de raios X)
12	Acompanhar o Ministério da Defesa, a polícia e a marinha para melhorar os procedimentos operacionais normalizados e o planeamento da resposta a emergências (em terra e na água)
13	Reforçar a relação entre as diferentes partes interessadas dos portos internacionais.
14	Melhorar a legislação, as práticas e os procedimentos nacionais em matéria de cibersegurança portuária
15	Avaliação da cibersegurança e gestão da cibersegurança
16	Estabelecer, aplicar, auditar e melhorar continuamente o plano de cibersegurança
17	Nomear um responsável pela cibersegurança e uma equipa de cibersegurança
18	Instalar um Comité de Segurança Portuária
19	Colaborar/estabelecer e operar um SOC
20	Organizar um grupo de gestão diária para tratar de incidentes e outras tarefas diárias de cibersegurança
21	Formação do pessoal de segurança (operadores de segurança)
22	Formação para a gestão da segurança (PFSO, PSO)
23	Formação do pessoal informático envolvido na segurança dos sistemas informáticos

9.13. Recomendações para a UE: Rumo a uma colaboração estável entre a UE e África

Uma colaboração UE-África nos seguintes domínios reforçaria a segurança marítima mundial e a segurança das nossas cadeias de abastecimento:

- *Criar colaborações estáveis* entre os Ministérios dos Transportes Marítimos, as agências de segurança e os ISACS marítimos para chegar a um entendimento comum, monitorizar continuamente, atenuar os desafios de segurança e os incidentes de segurança transfronteiriços no ecossistema marítimo. Criar sinergias fortes e trocar conhecimentos, recomendações e melhores práticas.
- *Campanhas de sensibilização e formação no domínio da proteção do transporte marítimo*: Estabelecer uma colaboração com entidades públicas e privadas para criar centros de sensibilização para a proteção do transporte marítimo, de formação operacional e de formação em matéria de gestão de incidentes, tendo em vista as necessidades gerais de proteção do transporte marítimo e do transporte marítimo, em que as plataformas de simulação e de exercícios facilitariam o desenvolvimento de competências.

- *Colmatar a lacuna de cibercompetências* com avaliações de risco práticas, simulação virtual de ataques e incidentes industriais dirigidos ao sector do transporte marítimo e ao ecossistema digital geral da cadeia de abastecimento marítimo e internacional. A utilização extensiva de ciberespaços pode ajudar as partes interessadas do sector do transporte marítimo a melhorar a sua compreensão no tratamento de ataques e incidentes complexos e a melhorar a preparação e a resiliência no sector do transporte marítimo. Tal implicaria experiências realistas baseadas em dados concretos e exercícios de "captura da bandeira" com equipas de cibersegurança e de ataque confrontadas umas com as outras. A Associação Internacional das Sociedades de Classificação (IACS) e a IMO podem basear-se na experiência da ENISA-Cyber Europe e continuar a colaborar com a ENISA e o CERT-EU para promover a formação em cibersegurança e preparar o caminho para uma formação eficaz no sector marítimo.
- *Apoio transfronteiriço no funcionamento de SOC marítimos* que prevejam e gerem eficazmente ciberataques e incidentes de segurança.
- *Harmonizar os esforços de certificação marítima*: Auditar e avaliar conjuntamente a segurança do equipamento marítimo para garantir a privacidade, a segurança, a transparência, a interoperabilidade, a responsabilização e a conformidade com a legislação e as directrizes da UE e internacionais em matéria de segurança. Incentivar as comunidades da UE e de África (militares e civis) de fabricantes, criadores e integradores a adoptarem a cultura da partilha de responsabilidades em matéria de segurança, realizando testes de conformidade comuns utilizando normas internacionais.
- Efetuar regularmente *avaliações comparativas* entre os portos da UE, da região da África Subsariana e de outras regiões do mundo, como o Sudeste Asiático. Tal seria útil para destacar as abordagens bem sucedidas da UE e de África em matéria de segurança e cibersegurança que podem ser reproduzidas noutras regiões.

10 Referências

Acharya, T. (2019, 31 de julho). *As caixas negras e a sua intrusão*. Disponível em Towards Data Science: https://towardsdatascience.com/black-boxes-and-their-intrusion-620aa3c4c56b

Centro de Cooperação de Tecnologia Marítima de África lançado em Mombaça. (2017, 13 de dezembro). Acedido em EEAS: https://www.eeas.europa.eu/node/37286_en

Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais. (2014). União Africana. Acedido em https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Progresso da cibersegurança marítima de África após o ataque à Transnet. (2021, 16 de setembro). Acedido em The Maritime Executive: https://maritime-executive.com/article/africa-s-maritime-cyber-security-progress-after-transnet-attack

Alcaide, J. I., & Garcia-Llave, R. (2020). A cibersegurança das infraestruturas críticas e o sector marítimo. *Transportation Research Procedia, 45*, 547-554. doi:10.1016/j.trpro.2020.03.058

Alderton, P. (1999). *Port Management and Operations.* LLP Professional Publishing.

Ashraf, I., Park, Y., Hur, S., Kim, S., Alroobaea, R., Bin Zikria, Y., & Nosheen, S. (2022). Uma pesquisa sobre ameaças à segurança cibernética na indústria marítima habilitada para IoT. *IEEE Transactions on Intelligent Transportation Systems*, 1-14. doi:10.1109/TITS.2022.3164678

Unidades do Espaço Atlântico. (s.d.). Disponível em United States Coast Guard Atlantic Area: https://www.atlanticarea.uscg.mil/Our-Organization/Area-Units/

Burt, J. (2021, 10 de agosto). Cenário de cibersegurança e ameaças às operações marítimas. Acedido em https://www.tenntom.org/wp-content/uploads/2021/10/CISA-Jason-Burt_CISA_Cybersecurity-Port_Maritime-Security.pdf

Hackers da China roubam dados de empreiteiro da Marinha dos EUA - relatórios. (2018, junho 9). Acedido em BBC: https://www.bbc.com/news/world-us-canada-44421785

Código de práticas seguras para a estiva e fixação da carga (Código CSS). (s.d.). Acedido em IMO: https://www.imo.org/en/OurWork/Safety/Pages/CSS-Code.aspx

Company, R. (2017, 21 de julho). *Como os portos podem proteger-se contra as ameaças à segurança cibernética e física*. Acedido em Medium: https://medium.com/@ICHCA/how-ports-can-protect-themselves-against-cyber-and-physical-security-threats-b6bd10c4f7a7

Costa Concordia: O que aconteceu. (2015, 10 de fevereiro). Acedido em BBC: https://www.bbc.co.uk/news/world-europe-16563562

Coulibaly, S., Kassa, W., & Zeufack, A. (2022, junho). *Reengenharia do comércio africano com a União Europeia e os Estados Unidos: O sucesso requer reformas em ambos os lados*. Acedido em Blogs do Banco Mundial: https://blogs.worldbank.org/africacan/re-engineering-african-trade-european-union-and-united-states-success-requires-reform

Darbra, R.-M., & Casal, J. (2004, fevereiro). Análise histórica dos acidentes em portos marítimos. *Safety Science, 42*(2), 85-98. doi:10.1016/S0925-7535(03)00002-X

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (2016). Acedido em https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Drougkas, D. A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019, 26 de novembro). *Port Cybersecurity - Boas práticas para a cibersegurança no sector marítimo.* ENISA. Acedido em ENISA: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Cenário de Ameaças ENISA 2022. (2022). Agência da União Europeia para a Cibersegurança (ENISA). Acedido em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Erstad, E., Ostnes, R., & Lund, M. (2021, março). Uma abordagem operacional para a resiliência cibernética marítima. *TransNav, 15*(1). doi:10.12716/1001.15.01.01

ESPO: The First Port of Call for European Transport Policy Makers in Brussels. (s.d.). Acedido em ESPO: https://www.espo.be/

UE-África: Pacote de Investimento Global Gateway. (s.d.). Acedido em Comissão Europeia: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

Agência Europeia da Segurança Marítima . (s.d.). Acedido em EMSA: https://www.emsa.europa.eu/

Agência da União Europeia para a Cibersegurança (ENISA). (2020). Cenário de ameaças da ENISA: 15 principais ameaças em 2020. Acedido em https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

Guia de Boas Práticas: Cibersegurança para portos e sistemas portuários. (2020). The Institution of Engineering and Technology. Acedido em 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

Uma participação maior e mais diversificada no comércio global é fundamental para alcançar a transformação económica de África, afirma o novo livro do Banco Mundial. (2022, fevereiro 10). Acedido em 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, 22 de agosto). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History [A história não contada de NotPetya, o ataque cibernético mais devastador da história]*. Acedido em Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Orientações - Gestão do risco cibernético para os portos. (2020). Agência da União Europeia para a Cibersegurança (ENISA). Acedido em https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Orientações sobre a gestão do ciber-risco marítimo. (2017). Londres: IMO. Acedido em https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf

Mapa do Golfo da Guiné. (2021, fevereiro 10). Instituto de Estudos de Segurança. Acedido em https://issafrica.s3.amazonaws.com/site/images/2021-02-10-gulf-of-guenea-piracy-map.png

Hand, M. (2020, 17 de abril). *MSC confirma que ataque de malware causou interrupção do site*. Acedido em Seatrade Maritime News: https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage

Desastre do Ferry Herald of Free Enterprise - 1987. (s.d.). Acedido em Devastating Disasters: https://devastatingdisasters.com/herald-of-free-enterprise-ferry-disaster-1987/

OIT: Organização Internacional do Trabalho. (s.d.). Acedido em UN: Gabinete do Enviado do Secretário-Geral para a Juventude: https://www.un.org/youthenvoy/2013/08/ilo-international-labour-organization/?gclid=CjwKCAiAv9ucBhBXEiwA6N8nYF5eTI5UjefYhsbZBgjQa8jYr3hWW0MocPuYj4mAk-nPawYFcgjb1hoCS3QQAvD_BwE

Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS), 1974. (s.d.). Acedido em IMO: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

Convenção Internacional sobre Normas de Formação, Certificação e Serviço de Quartos para os Marítimos, 197. (s.d.). Acedido em IMO: https://www.imo.org/en/OurWork/HumanElement/Pages/STCW-Convention.aspx

Inventário de Métodos e Ferramentas de Gestão de Riscos / Avaliação de Riscos . (s.d.). Acedido em Agência Europeia para a Cibersegurança (ENISA): https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory

ISO/IEC 27001 e normas conexas: Gestão da segurança da informação. (s.d.). Acedido em ISO: https://www.iso.org/isoiec-27001-information-security.html

Jørgensen, R. N. (2018). *Inquérito sobre cibersegurança mostra que é necessária mais ação na indústria*. Acedido em BiMCO: https://www.bimco.org/news/priority-news/20180924-cyber-security-survey

Kalogeri, E., & Polemi, N. (2022). Uma taxonomia das normas de segurança marítima. *6ª Conferência NMIOTC sobre Segurança Cibernética no Domínio Marítimo.* Baía de Souda: NATO.

Kioskli, K., & Polemi, N. (2020). Uma abordagem sócio-técnica para a avaliação do risco cibernético. *Revista Internacional de Engenharia Eletrotécnica e de Computadores, 14*(10), 305-309. Acedido em https://publications.waset.org/10011507/a-socio-technical-approach-to-cyber-risk-assessment

Kioskli, K., & Polemi, N. (2020). Abordagem psicossocial para inteligência de ameaças cibernéticas. *Jornal Internacional de Computação Caótica, 7*(1), 159-165. doi:10.20533/ijcc.2046.3359.2020.0021

Langewiesche, W. (2004, maio). Uma história do mar. *The Atlantic*. Acedido em https://www.theatlantic.com/magazine/archive/2004/05/a-sea-story/302940/

Comércio marítimo e África. (2018, 3 de outubro). Acedido em UNCTAD: https://unctad.org/press-material/maritime-trade-and-africa

Medidas para reforçar a proteção do transporte marítimo: Orientações de cibersegurança da IAPH para portos e instalações portuárias. (2021). IMO. Acedido em 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, setembro). Uma análise retrospetiva de incidentes de segurança cibernética marítima. *TransNav, 15*(3). doi:10.12716/1001.15.03.04

MTCC África. (s.d.). Acedido em MTCC Africa: http://mtccafrica.jkuat.ac.ke/

Negreiro, M. (2022). *A Diretiva NIS2: Um elevado nível comum de cibersegurança na UE.* Acedido em https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Quadro de Gestão de Riscos do NIST (RMF). (s.d.). Acedido em NIST: Centro de Recursos de Segurança Informática: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#/

O nosso trabalho. (s.d.). Acedido em IMO: https://www.imo.org/en/OurWork/Pages/Default.aspx

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

Porto de San Diego: e-mails de phishing continuam entre as maiores ameaças cibernéticas. (2021, 19 de agosto). Acedido em 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.

Resolução A.682 (17). (1991). Organização Marítima Internacional. Acedido em https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.682(17).pdf

Reva, D. (2020). *Cibersegurança marítima: Preparar África.* Instituto de Estudos de Segurança. Acedido em https://issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf

Livro de Regras 2021. (s.d.). UKP&I. Acedido em https://www.ukpandi.com/news-and-resources/rulebook-2021/

Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports. (s.d.). Acedido em CORDIS: https://cordis.europa.eu/project/id/740477

Shapira, I. (2006, 4 de janeiro). Capitão culpado de explosão fatal de petroleiro ao largo de Va. *The Washington Post*. Acedido em 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 e o Código ISPS. (s.d.). Acedido em IMO: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

Normas. (s.d.). Acedido em ISO: https://www.iso.org/standards.html

Reforçar as portas de entrada de África para o comércio. (2018). PwC. Acedido em https://www.pwc.co.za/en/assets/pdf/strengthening-africas-gateways-to-trade.pdf

A Explosão do Porto de Beirute. (s.d.). Acedido em Forensic Architecture: https://forensic-architecture.org/investigation/beirut-port-explosion

Directrizes sobre cibersegurança a bordo dos navios - Versão 4 (2020). BIMCO. Acedido em https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

O Código Internacional de Gestão da Segurança (ISM). (s.d.). OMI. Acedido em https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

Cenário de ameaças para ataques à cadeia de abastecimento. (2021). Agência da União Europeia para a Cibersegurança (ENISA). Acedido em https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Titanic. (s.d.). Acedido em Britannica: https://www.britannica.com/topic/Titanic/Aftermath-and-investigation#ref302525

Tomter, L., & Gundersen, M. (2019, 14 de abril). *IT-sjefen i Hydro om dataangrepet: - Man tror krisen blir stor, så blir den enda verre*. Acedido em 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. (s.d.). Acedido em Strengthening the security and safety of ports in West and Central Africa : https://wecaps.eu/en/

Widup, S. (2019). *Relatório de investigações de violação de dados da Verizon de 2019.* Verizon. Acedido em https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf

Winder, D. (2019, julho). *A Guarda Costeira dos EUA emite alerta após o navio que vai para o porto de Nova York ser atingido por um ataque cibernético*. Acedido em 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: Questionários de segurança

11.1. Anexo A: Questionário de sensibilização para a governação da segurança

Com base na norma ISO27001[72], o questionário seguinte pode servir para avaliar a estrutura de governação de uma empresa marítima para gerir os riscos de segurança:

Objetivo de controlo	Tema	Questão	Não	Sim
Política de segurança (segurança e cibersegurança)	Política de segurança da informação	O pessoal tem conhecimento da política de segurança associada às suas funções?		
Organização da segurança	Organização interna	O pessoal está consciente das suas responsabilidades em matéria de segurança?		
		O pessoal possui as autorizações necessárias?		
	Partes externas	O pessoal está consciente dos possíveis riscos quando lida com entidades externas?		
		O pessoal está a tomar medidas de segurança quando lida com os clientes?		
Gestão de activos	Responsabilidade pelos activos	O pessoal tem conhecimento dos activos com que está a lidar?		
		O pessoal tem conhecimento da propriedade destes activos?		
		O pessoal tem conhecimento da utilização dos activos?		
	Classificação da informação	O pessoal tem conhecimento das directrizes de classificação?		
		O pessoal tem conhecimento das informações relativas à rotulagem e ao manuseamento?		
Segurança dos recursos humanos	Durante o emprego	O pessoal conhece as suas responsabilidades de gestão?		
		O pessoal recebeu formação sobre temas de sensibilização em matéria de segurança (por exemplo, medidas de controlo do acesso) e cibersegurança (por exemplo, phishing, engenharia social, armazenamento de dados)?		

[72] Da Organização Internacional de Normalização (ISO); https://www.iso.org/isoiec-27001-information-security.html

	Rescisão do contrato de trabalho	O pessoal sabe que, após a cessação do contrato de trabalho, tem de devolver os seus activos e os direitos de acesso são retirados?		
Segurança física e ambiental	Áreas seguras	O pessoal tem conhecimento do perímetro de segurança física do porto?		
		O pessoal tem conhecimento dos controlos físicos de entrada?		
		O pessoal tem conhecimento do procedimento de segurança do local de trabalho?		
	Segurança do equipamento	O pessoal tem conhecimento da utilização do equipamento de segurança e informático existente nas instalações?		
		O pessoal tem conhecimento da política de "trazer o seu próprio dispositivo"?		
		O pessoal tem conhecimento dos procedimentos relativos à eliminação ou reutilização segura do equipamento?		
Gestão das comunicações e das operações	Procedimentos operacionais e responsabilidades	O pessoal tem conhecimento dos procedimentos operacionais relacionados com as actividades?		
		O pessoal está a par do processo de gestão da mudança?		
	Proteção contra código malicioso e móvel	O pessoal tem conhecimento dos controlos contra códigos maliciosos (ou seja, tratamento de mensagens de correio eletrónico)?		
		O pessoal tem conhecimento dos controlos contra o código móvel (ou seja, dispositivos móveis infectados)?		
	Apoio	O pessoal tem conhecimento do processo de cópia de segurança das informações?		
	Tratamento dos meios de comunicação social	O pessoal tem conhecimento da gestão dos suportes amovíveis?		
		O pessoal tem conhecimento da eliminação dos suportes de informação?		

		O pessoal tem conhecimento dos procedimentos de tratamento da informação?		
		O pessoal tem conhecimento da segurança da documentação do sistema?		
	Intercâmbio de informações	O pessoal tem conhecimento da proteção dos suportes físicos em trânsito?		
		O pessoal tem conhecimento das mensagens electrónicas?		
	Serviços marítimos electrónicos	O pessoal tem conhecimento do procedimento relativo às transacções em linha e à utilização de informações publicamente disponíveis?		
	Controlo	O pessoal tem conhecimento da política relativa aos registos?		
Controlo de acesso	Requisitos comerciais para o controlo de acesso	O pessoal tem conhecimento da política de controlo de acesso?		
	Gestão do acesso dos utilizadores	O pessoal tem conhecimento do procedimento de registo do utilizador?		
		O pessoal tem conhecimento da política/gestão das palavras-passe dos utilizadores?		
		O pessoal tem conhecimento do procedimento relativo aos direitos de acesso dos utilizadores?		
	Responsabilidades do utilizador	O pessoal tem conhecimento da utilização da palavra-passe?		
		O pessoal tem conhecimento do procedimento relativo ao equipamento de utilizador sem vigilância?		
		O pessoal tem conhecimento da política de "secretária limpa e ecrã limpo"?		
	Controlo de acesso à rede	O pessoal tem conhecimento da política de utilização dos serviços de rede?		

	Controlo de acesso ao sistema operativo	O pessoal tem conhecimento dos procedimentos de início de sessão seguro?		
		O pessoal tem conhecimento da utilização dos utilitários do sistema?		
	Controlo do acesso a aplicações e informações	O pessoal tem conhecimento das restrições de acesso à informação?		
		O pessoal tem conhecimento da proteção do isolamento de sistemas sensíveis?		
	Computação móvel e teletrabalho	O pessoal tem conhecimento da política aplicável em matéria de utilização de computadores e comunicações móveis?		
		O pessoal tem conhecimento da política de utilização das tecnologias do porto/navio e dos sistemas de teletrabalho?		
Aquisição, desenvolvimento e manutenção de sistemas de informação	Controlos criptográficos	O pessoal tem conhecimento da política relativa à utilização de chaves criptográficas e equipamento conexo?		
Gestão de incidentes de segurança da informação	Comunicação de eventos e deficiências de segurança da informação	O pessoal tem conhecimento dos procedimentos de comunicação de eventos de segurança da informação?		
		O pessoal tem conhecimento dos procedimentos de comunicação de deficiências de segurança?		
Gestão da continuidade das actividades	Gestão da continuidade das actividades	O pessoal tem conhecimento do plano de continuidade das actividades e do plano de recuperação de desastres relacionado com as funções?		

11.2. Anexo B: Questionário sobre práticas de segurança

O questionário que se segue pode ser distribuído aos portos para avaliar a maturidade das suas práticas de cibersegurança. Pode também ser distribuído às companhias marítimas e aos armadores para que estes comuniquem e avaliem as práticas de segurança implementadas e seguidas:

Questionário aos portos e operadores marítimos sobre a sensibilização para a segurança

Informações (facultativo)

Empresa	xxxxxx
Nome	xxxxx
Posição	xxxxx
Número de empregados	xxxxx
Atividade empresarial	xxxx
url	xxxxx
correio eletrónico	xxxxxx

Data

Caro interveniente do sector marítimo,

O objetivo deste questionário é compreender o nível de sensibilização para a segurança da infraestrutura crítica (IC) marítima em termos de ameaças e vulnerabilidade de todos os níveis da IC, ou seja, (a) infraestrutura física, (b) equipamento da infraestrutura de telecomunicações (c) software (d) serviços e aplicações (e) dados (f) utilizadores (pessoas e coisas externas/internas). Além disso, procurar-se-á obter uma panorâmica dos serviços e dos utilizadores em termos de vulnerabilidade.
O questionário pretende identificar se:

- Os operadores marítimos estabeleceram um plano de segurança (plano de segurança portuária e política de segurança das TIC), em que medida é aplicado e quais os seus objectivos;
- Os empregados e utilizadores do sector marítimo estão conscientes das questões de segurança relacionadas com as suas actividades diárias;
- A formação de sensibilização para a segurança da informação é oferecida, bem como a sua eficácia;
- Existem inter-relações entre as autoridades competentes e as IC marítimas (por exemplo, portos) e por que razões.

Para efeitos do presente inquérito, apenas são consideradas as IC marítimas na sua qualidade de operadores (ou seja, portos que são simultaneamente proprietários e operadores OU operadores de terminais). Embora o inquérito incida sobre os portos, aplica-se a qualquer IC marítima.

As respostas serão consideradas confidenciais e apenas serão comunicados os valores agregados.

Para mais informações, contactar:

xxxxxx

Plano de segurança do porto

1. O porto dispõe de um plano de gestão da segurança bem definido?

- ◻ Sim - passar às pergunt 1a
- ◻ Não - passar à pergunta 2

1a. Qual é o modelo de gestão da segurança que adopta? [Escolha apenas um]

◻	Internamente - por exemplo, de um departamento específico ou pessoa(s) do porto (por exemplo, PFSO)
◻	Externalizar - por exemplo, outra empresa ou organização ou perito(s) externo(s)
◻	Outros

1b. O que melhor descreve a sua perceção da segurança: [Escolha apenas um]

◻	Não diz respeito/influencia as suas actividades empresariais
◻	Não é a sua primeira prioridade, mas tenciona considerá-la no futuro
◻	Compreende a sua necessidade, mas é demasiado caro para a considerar

1c. Que regimes de segurança abrange o seu plano de segurança? [Selecionar tantos quantos os adequados]

◻	ISPS
◻	ISO 9001, ISO 14001 (Serviços de portos de cruzeiro)
◻	ISO 27001
◻	ISO 27002
◻	ISO 28000
◻	Outros: PERS (Sistema de Revisão Ambiental Portuária, para toda a zona portuária)
◻	Outros (especificar:_____)

1d. O seu sistema de segurança identifica e analisa em profundidade os seguintes aspectos?

Actividades	O nosso plano de segurança não cobre isto.	O nosso Plano de Segurança cobre-o, e...	
		os interessados apresentam documentos válidos, mas nós não os analisamos.	mantemos uma base de dados ativa sobre os mesmos e dispomos de processos específicos e pormenorizados para as análises.
Planos de proteção dos navios	◻	◻	◻
Agentes de proteção de navios	◻	◻	◻
Agentes de segurança da empresa	◻	◻	◻

Equipamento de bordo	☐	☐	☐
Planos de segurança das instalações portuárias correspondentes	☐	☐	☐
Agentes de segurança de instalações portuárias	☐	☐	☐
Determinados equipamentos de segurança	☐	☐	☐
Alguns elementos de segurança	☐	☐	☐
Controlo das actividades das pessoas e da carga	☐	☐	☐
Comunicações seguras	☐	☐	☐
Acesso seguro nos sectores portuários (monitorização, controlo)	☐	☐	☐
Política do ciberporto	☐	☐	☐
Outros (especificar)	☐	☐	☐
Não sei	☐		

2. Nos últimos 12 meses, teve em conta as questões de segurança nas seguintes actividades do porto? Em caso afirmativo, as suas reacções foram proactivas ou reactivas?

Actividades	As questões de segurança não foram consideradas	Sim, foram consideradas questões de segurança	
		Natureza da ação	
		proactivo	reativo
Melhorias nos seus serviços/produtos/negócios/cadeias de abastecimento	☐	☐	☐
Conformidade do sector	☐	☐	☐
Melhorias no funcionamento dos seus sistemas informáticos	☐	☐	☐
Melhorias no funcionamento dos sistemas de entrada/saída/perímetro das instalações portuárias	☐	☐	☐
Melhoria do perfil da sua empresa e do nível de confiança dos seus utilizadores e serviços	☐	☐	☐
Conformidade com a legislação da UE que influencia as suas operações internacionais e cadeias de abastecimento	☐	☐	☐
Privacidade e proteção de dados	☐	☐	☐
Segurança do pessoal e dos utilizadores	☐	☐	☐
Acesso seguro nos sectores portuários	☐	☐	☐
Não sei	☐		

3. Seleccione três (3) categorias principais de regulamentação/legislação que influenciam o seu funcionamento e as medidas de segurança nos últimos/próximos 12 meses. Indique se tem em conta algum projeto de segurança nas suas selecções.

Tipos de regulamentos	Nos últimos 12 meses	Nos próximos 12 meses	Projectos de segurança em curso/em estudo
Auditoria interna:			
ISPS	☐	☐	☐
ISM	☐	☐	☐
Famílias de normas ISO	☐	☐	☐
Famílias OHSAS 18000	☐	☐	☐
Sarbanes-Oxley	☐	☐	☐
Regulamento (CE) n.º 725/2004	☐	☐	☐
Normas SOLAS/MARPLE			
Diretiva do Conselho 2008/114/CE DO CONSELHO relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.	☐	☐	☐
Data Protection (e.g., GDPR,NIS, NISII, ISO 27000/27001/27002/27005, ISO15048, ISO18045)	☐	☐	☐
Regulamentos sectoriais (por exemplo, norma de segurança de dados PCI)	☐	☐	☐
Regulamentos das autoridades aduaneiras e financeiras	☐	☐	☐
Outros (Problemas com a alfândega _____)	☐	☐	☐
Outros (Sem problemas com as autoridades financeiras _____)	☐	☐	☐
Proteção de dados (por exemplo, RGPD, NIS, NISII, ISO 27000/27001/27002/ 27005, ISO15048, ISO18045)	☐	☐	☐
Outro (por favor definir_____)	☐	☐	☐

4. Seleccione cinco (5) questões de cibersegurança em termos de importância (1 = menor importância, 5 = maior importância) para a sua empresa. Tem um plano para resolver estas questões de segurança?

Questões de segurança em matéria de cibersegurança	Importante questão de segurança	Plano de resposta		
		Agora	Próximos 12 meses	Sem plano
Divulgação segura dos dados (às autoridades competentes, aos fornecedores da cadeia de abastecimento, às companhias marítimas, etc.)	☐	☐	☐	☐
Armazenamento seguro de dados	☐	☐	☐	☐
Acesso (físico) de/para as instalações portuárias	☐	☐	☐	☐
Serviços portuários seguros (gestão de contentores, GNL, serviços da cadeia de abastecimento)	☐	☐	☐	☐
Identificadores de radiofrequência (RFID)	☐	☐	☐	☐
Dispositivos móveis (por exemplo, PDA, telemóveis inteligentes)	☐	☐	☐	☐
Sistemas de controlo automatizado das fronteiras (ABC)	☐	☐	☐	☐
Armazenamento móvel (por exemplo, unidade flash USB, unidades portáteis)	☐	☐	☐	☐
Telefonia por voz sobre IP	☐	☐	☐	☐
Serviços Web	☐	☐	☐	☐
Redes sem fios	☐	☐	☐	☐
Comunicação segura por satélite	☐	☐	☐	☐
Novos sistemas operacionais	☐	☐	☐	☐
Criptografia das mensagens de correio eletrónico	☐	☐	☐	☐
Criptografia do disco rígido	☐	☐	☐	☐

Práticas de segurança

5. Como é que verifica o nível de segurança da sua empresa? [Escolha mais do que uma, se necessário]

☐	Auditoria Interna (do Departamento de Segurança)
☐	Auditoria externa
☐	Avaliação interna do pessoal
☐	Outros
☐	Não dispomos de tais procedimentos

6. Seleccione cinco (5) actividades principais de segurança em termos de importância (1 = menor importância, 5 = maior importância) para o seu porto. Seleccione, de forma

independente, cinco (5) actividades principais de segurança em termos do tempo de execução necessário (1 = pouco tempo, 5 = muito tempo):

	Importância	Tempo de implementação
Conformidade com o ISP	□	□
Conformidade com a norma ISO27001, 27005	□	□
Gestão da continuidade das actividades	□	□
Gestão do risco e da segurança	□	□
Prosseguir, desenvolver e integrar os sistemas informáticos	□	□
Gestão do controlo de acesso	□	□
Gestão de comunicações e operações	□	□
Segurança física	□	□
Proteção dos trabalhadores (segurança)	□	□
Actualizações de serviços e produtos	□	□
Gestão da segurança	□	□
Política de segurança (cibernética)	□	□
Privacidade - Proteção de dados	□	□
Responsabilidade Plano de recuperação de desastres	□	□

7. Como é que aborda/resolve os seguintes problemas de segurança no seu porto;

Questões de segurança:	Nenhuma consideração	Melhores práticas	Métodos próprios
Incidentes de cibersegurança - Ataques	□	□	□
Continuidade das actividades	□	□	□
Resiliência empresarial	□	□	□
Gestão do risco cibernético	□	□	□
Gestão do risco físico	□	□	□
Privacidade e proteção de dados	□	□	□
Mecanismos de segurança nos serviços electrónicos e portuários oferecidos	□	□	□

8. Quando colabora com outras empresas (por exemplo, subcontratação, contratantes externos, terceiros), quais das seguintes medidas considera necessárias em matéria de segurança?

□	Os seus colaboradores têm e seguem uma política de segurança auditável
□	Os seus colaboradores são obrigados a utilizar/respeitar a sua própria política de segurança e as suas preocupações de segurança
□	Os seus colaboradores estão em conformidade com a norma ISO 27001
□	Nenhuma das anteriores
□	Outros

9. Alguma vez efectuou uma avaliação dos riscos físicos?

- ☐ Sim
- ☐ Não

10. Com que frequência e a quem são comunicados os riscos e incidentes de segurança física?

	Frequência				
	Diário	Mensal	Trimestre	Semestre	Nunca
Oficial de segurança das instalações portuárias	☐	☐	☐	☐	☐
Empresa de segurança (externa)	☐	☐	☐	☐	☐
Polícia	☐	☐	☐	☐	☐
Alfândega	☐	☐	☐	☐	☐
Autoridades competentes (especificar:_____)	☐	☐	☐	☐	☐
Companhias de seguros	☐	☐	☐	☐	☐
Bancos e instituições financeiras	☐	☐	☐	☐	☐
Empreiteiros e partes interessadas	☐	☐	☐	☐	☐
Câmara de Comércio (ou organização similar)	☐	☐	☐	☐	☐
Autoridade Nacional de Certificação	☐	☐	☐	☐	☐
Outros (especificar _____)	☐	☐	☐	☐	☐
Outros (especificar _____)	☐	☐	☐	☐	☐
Outros (especificar _____)	☐	☐	☐	☐	☐

11. Já efectuou alguma vez uma avaliação do risco cibernético?

- ☐ Sim
- ☐ Não

12. Com que frequência comunica os riscos e incidentes de cibersegurança e a quem?

	Frequência				
	Diário	Mensal	Trimestre	Semestre	Nunca
Responsável pela cibersegurança portuária	☐	☐	☐	☐	☐
Empresa de segurança (externa)	☐	☐	☐	☐	☐
Autoridades públicas (por exemplo, polícia	☐	☐	☐	☐	☐
Empresa marítima	☐	☐	☐	☐	☐
Autoridades competentes (por exemplo, CERT, CSIRTS, ISAC, Ministério)	☐	☐	☐	☐	☐
Companhias de seguros	☐	☐	☐	☐	☐
Bancos e instituições financeiras	☐	☐	☐	☐	☐
Empreiteiros e partes interessadas	☐	☐	☐	☐	☐
OMI, EMSA (ou organização marítima similar)	☐	☐	☐	☐	☐
Autoridade Nacional de Certificação	☐	☐	☐	☐	☐
Outros (especificar _____)	☐	☐	☐	☐	☐
Outros (especificar _____)	☐	☐	☐	☐	☐

13. Como é que se informa sobre as questões de segurança? Que organização seria mais adequada para receber formação sobre segurança? Quais são os temas que mais lhe interessam? (Pode fazer várias escolhas)

	Tecnologias de segurança/ implementação	Políticas de segurança	Avaliação dos riscos	Privacidade - Proteção de dados
Organizações	☐	☐	☐	☐
Consultores de segurança (empresas privadas)	☐	☐	☐	☐
Universidade	☐	☐	☐	☐
Organismo nacional	☐	☐	☐	☐
Internet	☐	☐	☐	☐
Organismo governamental	☐	☐	☐	☐
Câmaras de Comércio	☐	☐	☐	☐
Associações do sector ou organismos profissionais (por exemplo, OMI, EMSA, ENISA, NIST)	☐	☐	☐	☐
Imprensa, publicações científicas	☐	☐	☐	☐

14. De que normas de segurança tem conhecimento?

ISO 9001	☐
ISPS	☐
ISM	☐
Inspecções SIRE / ATB	☐
ISA/IEC-62443	☐
Pedido de inspeção de barcaças e ATB terrestres dos EUA	☐
Inspeção EBIS	☐
ISO/IEC 2700x	☐
ISO 20858	☐
ISO 15408, ISO18045	☐
Fórum de Segurança da Informação	☐
CobIT	☐
Biblioteca de Infra-estruturas de Tecnologias da Informação (ITIL)	☐
Integração do Modelo de Maturidade das Capacidades (CMMI)	☐
SEISMED	☐
Nenhuma das anteriores	☐
Outros (especificar _____)	☐
Outros (especificar _____)	☐
Adicionar mais se necessário	☐

15. Qual é a situação do seu porto no que respeita às seguintes actividades de segurança?

Atividade	Em vigor/ Em progresso	Em vigor nos próximos 12 meses	Não planeado
Acesso físico através de cartões inteligentes	☐	☐	☐
Acesso físico com cartões de identificação em papel	☐	☐	☐
Acesso físico através de sistemas automatizados de controlo de fronteiras (ABC)	☐	☐	☐
Utilização de diferentes tecnologias de autenticação para o acesso físico (por exemplo, cartões de proximidade, cartões inteligentes, biometria)	☐	☐	☐
Utilização de sistemas de deteção de intrusão	☐	☐	☐
Filtros antivírus e anti-spam actualizados	☐	☐	☐
Utilização de firewalls	☐	☐	☐
Inspecções (fora do prazo) de navios	☐	☐	☐