ABEPH · ABRATEC Associação Brasileira dos Terminais de Contêineres · ABTL Associação Brasileira de Terminais de Líquidos · ABTRA Associação Brasileira de Terminais e Recintos Alfandegados · ABTP Associação Brasileira dos Terminais Portuários · ATP Associação de Terminais Portuários Privados · FENOP Federação Nacional das Operações Portuárias

GUIA DE MELHORES PRÁTICAS DE SEGURANÇA
PORTUÁRIA E ADUANEIRA

EDUFMA

Organização
Prof. Dr. SÉRGIO CUTRIM

GUIA DE MELHORES PRÁTICAS DE SEGURANÇA
PORTUÁRIA E ADUANEIRA

EDUFMA

GUIA DE MELHORES PRÁTICAS DE SEGURANÇA

PORTUÁRIA E ADUANEIRA

APOIO INSTITUCIONAL

CNT / SEST SENAT / ITL

Sistema Transporte

Capa — Dyego Santos Nolasco
Proj. Gráfico e Diagramação — Carlos Eduardo Sales
Revisão — Regysane Botelho Cutrim Alves

Dados Internacionais de Catalogação na Publicação (CIP)

G943 Guia de melhores práticas de segurança portuária e aduaneira [recurso eletrônico] / organização: Sérgio Cutrim ... [et al.]. – São Luís: EDUFMA, 2026.
143 P . :il.

ISBN 978-65-5363-532-6
1. Portos – Medidas de segurança. 2. Portos – Administração. 3. Administração alfandegária. I. Cutrim, Sérgio.

CDD (1. ed.) 363.123
CDU 656.615(81):34

Bibliotecária:
Tatyane Barbosa Philippi
CRB 14/735

IMPRESSO NO BRASIL [2026]

| EDUFMA | EDITORA DA UNIVERSIDADE FEDERAL DO MARANHÃO
Av. dos Portugueses, 1966 | Vila Bacanga
CEP: 65080-805 | São Luís | MA | Brasil
Telefone: (98) 3272-8157
www.edufma.ufma.br | edufma.sce@ufma.br

EQUIPE TÉCNICA

Prof. Dr. Sérgio Cutrim

▪ Doutor em Engenharia Naval e Oceânica pela Universidade de São Paulo. É administrador, professor e pesquisador com foco no setor portuário nos temas planejamento, governança e sustentabilidade. Professor da Universidade Federal do Maranhão. Coordenador do Laboratório de Pesquisa LabPortos, do Observatório Portuário e da Especialização em Gestão Portuária.

Antonio Russo Filho

▪ Bacharel em Economia e em Direito. Mestre em Engenharia pela USP. Trabalhou 33 anos como Auditor Fiscal da RFB, exercendo suas atividades nas Alfândegas de Manaus e do Porto de Santos. Desde maio de 2014 presta consultoria aduaneira nas atividades de logística de comércio exterior. Especialista em análise de risco ISO 31000. Auxilia empresas na adequação aos requisitos de Alfandegamento, compliance aduaneiro e Programa Operador Econômico Autorizado - OEA da Receita Federal do Brasil. Foi Coordenador do Programa CSI (Container Security Initiative) do acordo Brasil x Estados Unidos, no Porto de Santos, no período de 2005 a 2014, representando a RFB nas Conferências Internacionais em Washington. Foi membro da Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis do Estado de São Paulo (CESPORTOS), representando a Receita Federal do Brasil, no período de 2004 a 2014. Foi conselheiro convidado do CAP (Conselho de Administração Portuária do Porto de Santos), representando a Alfândega da Receita Federal do Brasil do Porto de Santos, no período de 2009 a 2013. Representou a Alfândega no Comitê de Infraestrutura e Logística do Porto de Santos, no período de 2008 a 2013.

Benjamim Vieira Paiva

▪ Profissional com mais de 15 anos de experiência nos setores portuário, logística e comunicação institucional. Atua como Consultor Portuário Independente, com foco em análise de stakeholders, planejamento setorial, elaboração de relatórios estratégicos e pesquisas técnicas aplicadas à governança de complexos logísticos. Possui trajetória consolidada no Porto do Itaqui, abrangendo gestão operacional, atendimento ao usuário, comunicação institucional, qualidade, certificações e relacionamento com clientes públicos e privados. Administrador com pós-graduação em Engenharia de Produção, com ampla vivência em planejamento, negociação, melhoria de processos e articulação com stakeholders.

Carlos Albuquerque

▪ Cientista Naval, Mestre em Engenharia de Produção na área de Pesquisa Operacional (UFPE) e Doutorando em Computação (UFF/RJ). Exerce a função de DPO no Cluster Tecnológico Naval do RJ. Exerceu as funções de Secretário Executivo e Coordenador da CESPORTOS/RJ. Coautor da Metodologia ARESP. Especialista em Inteligência e Transformação Digital. Pesquisador no LabPortos e no Observatório de Segurança Marítima nos temas Proteção de Infraestruturas Críticas, Segurança Portuária e Risco Cibernético. Professor na Academia Nacional de Polícia, e na FIA Business School. Formação complementar em Operações de Inteligência, Gerenciamento de Crises (COT/PF) e Auditoria pela Conportos/MJSP.

Elessandra Lira

▪ É advogada, atualmente atua no jurídico interno de Terminal Portuário nas áreas de contratos, seguros e riscos em Portos e Logística e societário. MBA em Gestão Jurídica Aduaneira e Internacional – Massachusetts Institute of Business/Harvard Business School. Mediadora Maritime Affairs pela Universidade de Coimbra. Trade Compliance Officer pelo Instituto de Comércio Internacional do Brasil, especialista em Direito Tributário pela Escola Brasileira de Direito, e Pós-graduanda em Direito Societário. Analista de Importação e Exportação pela Aduaneiras/RJ. Membra da Wista Brazil, Amecomex Brazil e Comissão de Direito Marítimo, Portuário e Aduaneiro da OAB Seccional São Paulo/SP.

Luciana Fuschini Nave

▪ Delegada de Polícia Federal aposentada, tendo exercido ao longo de sua carreira as funções de chefe da Delegacia da Polícia Federal em Santos e Coordenadora da CESPORTOS no estado de São Paulo. Auditora credenciada pela CONPORTOS, atua com consultoria em segurança empresarial e portuária, ISPS CODE, gestão de riscos e treinamentos. É graduada em Direito pela UNISANTOS e pós-graduanda em neurociência e comportamento pela PUC, além de possuir formação como Conselheira de Administração pelo IBGC.

LISTA DE ILUSTRAÇÕES

Figura 1 - Análise SWOT 22
Figura 2 - Processo de elaboração do Guia 26
Figura 3 - Etapas propostas para a aplicação estruturada do Guia 29
Figura 4 - Estrutura sistêmica da segurança portuária e aduaneira no Brasil 51
Quadro 1 – Tipo de ataques 82

SIGLAS

SIGLA	SIGNIFICADO
ABEPH	Associação Brasileira das Entidades Portuárias e Hidroviárias
ABRATEC	Associação Brasileira de Terminais de Contêineres
ABTL	Associação Brasileira de Terminais de Líquidos
ABTP	Associação Brasileira dos Terminais Portuários
ABTRA	Associação Brasileira de Terminais e Recintos Alfandegados
AD	Active Directory (Servidor de Identidade)
ADE	Ato Declaratório Executivo
ADM	Armas de Destruição em Massa
ANTAQ	Agência Nacional de Transportes Aquaviários
ANTT	Agência Nacional de Transportes Terrestres
ANVISA	Agência Nacional de Vigilância Sanitária
API	Application Programming Interface
APT	Advanced Persistent Threat (Ameaça Persistente Avançada)
ARESP	Análise de Risco com ênfase em Segurança Portuária
ATP	Associação de Terminais Portuários Privados
C-TPAT	Customs-Trade Partnership Against Terrorism
CAP	Conselho de Administração Portuária
CBP	Customs and Border Protection (Aduana dos EUA)
CDD	Classificação Decimal de Dewey
CDU	Classificação Decimal Universal
CESPORTOS	Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis
CFTV	Circuito Fechado de Televisão
CLP	Certificado de Livre Prática
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
COANA	Coordenação-Geral de Administração Aduaneira
COBIT	Control Objectives for Information and Related Technology
CONPORTOS	Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis
COT	Comando de Operações Táticas (da Polícia Federal)
COTEC	Coordenação Geral de Tecnologia e Segurança da Informação
CSF	Cybersecurity Framework (NIST)
CSI	Container Security Initiative
DC	Declaração de Cumprimento
DDoS	Distributed Denial of Service (Ataque de Negação de Serviço Distribuído)
DNS	Domain Name System
DPO	Data Protection Officer
DU-E	Declaração Única de Exportação
EAR	Estudo de Avaliação de Riscos
ENISA	Agência da União Europeia para Cibersegurança
ERM	Enterprise Risk Management (Gerenciamento de Riscos Corporativos)
ETC	Estação de Transbordo de Carga
FBI	Federal Bureau of Investigation

FENOP	Federação Nacional das Operações Portuárias
GRC	Governança, Risco e Conformidade
IA	Inteligência Artificial
IBGC	Instituto Brasileiro de Governança Corporativa
IDS	Intrusion Detection System
IMDG Code	International Maritime Dangerous Goods Code
IMO	International Maritime Organization (Organização Marítima Internacional)
IP4	Instalação Portuária Pública de Pequeno Porte
IPS	Intrusion Prevention System
IPTur	Instalação Portuária de Turismo
ISO	International Organization for Standardization
ISPS Code	International Ship and Port Facility Security Code
MAPA	Ministério da Agricultura, Pecuária e Abastecimento
MJSP	Ministério da Justiça e Segurança Pública
MPOR	Ministério de Portos e Aeroportos
MSC	Maritime Safety Committee (da IMO)
NCM	Nomenclatura Comum do Mercosul
NEPOM	Núcleo Especial de Polícia Marítima
OEA	Operador Econômico Autorizado
OMA	Organização Mundial das Aduanas
OMC	Organização Mundial do Comércio
ONU	Organização das Nações Unidas
OS	Organizações de Segurança
P&D	Pesquisa e Desenvolvimento
PDTI	Plano Diretor de Tecnologia da Informação
PF	Polícia Federal
PNSPP	Plano Nacional de Segurança Pública Portuária
PSI	Política de Segurança da Informação
PSP	Plano de Segurança Portuária
REDEX	Recinto Especial para Despacho Aduaneiro de Exportação
RFB	Secretaria Especial da Receita Federal do Brasil
RSI	Regulamento Sanitário Internacional
SGSI	Sistema de Gestão de Segurança da Informação
SISCOMEX	Sistema Integrado de Comércio Exterior
SOLAS	International Convention for the Safety of Life at Sea
SSC	Ship Sanitation Certificate
TCU	Tribunal de Contas da União
TRF4	Tribunal Regional Federal da 4ª Região
TRIPS	Trade-Related Aspects of Intellectual Property Rights
TUP	Terminal de Uso Privado
UNODC	United Nations Office on Drugs and Crime
UTM	Unified Threat Management

SUMÁRIO

1. **Introdução** 14

2. **Metodologia** 20

3. **Diretrizes para a aplicação do guia** 28

4. **Legislação aplicada** 33

   4.1 Segurança portuária 35
   4.2 Segurança aduaneira 37

5. **Atribuições na segurança portuária e aduaneira** 42

   5.1 Portuária 43
   5.1.1 Polícia federal 43
   5.1.2 Conportos e cesportos 44
   5.1.3 Supervisores de segurança portuária 46
   5.2 Aduaneira 46

6. **Principais atores** 50

7. **Ameaças e fraquezas na segurança portuária e aduaneira** 59

   7.1 Terrorismo e sabotagem 61
   7.1.1 Casos de terrorismo registrados no Brasil 61
   7.1.2 Ameaças e riscos em infraestruturas críticas 62
   7.1.3 Incidente no porto de vila do conde (barcarena/pa) 63
   7.1.4 Prevenção e resposta no setor portuário 64
   7.1.5 Sabotagem e riscos internos 66
   7.2 Passageiros clandestinos 69
   7.3 Roubo, furto de carga e extorsão 71
   7.4 Tráfico, descaminho e contrabando 75
   7.5 Espionagem industrial 78
   7.6 Treinamento inadequado 80
   7.7 Ciberataque 80

8. Melhores práticas de segurança (forças) 87
8.1 Melhores práticas no combate ao terrorismo e sabotagem 90
8.2 Melhores práticas para lidar com passageiros clandestinos 95
8.3 Melhores práticas no combate ao roubo, furto e extorsão 97
8.4 Melhores práticas no combate ao tráfico, descaminho e contrabando 103
8.5 Melhores práticas no combate à espionagem industrial 109
8.6 Melhores práticas para mitigar treinamentos inadequados 111
8.7 Melhores práticas no combate ao ciberataque 112

9. Oportunidades à segurança 121
9.1 Cooperação interagências 122
9.2 Cooperação entre o público e privado 124
9.3 Políticas públicas e financiamento 126

10. Conclusão 128

Referências 131

Anexo A 139

1- Introdução

Este guia foi desenvolvido sob a coordenação da Associação de Terminais Portuários Privados (ATP), em parceria com a Universidade Federal do Maranhão (UFMA), por meio do Laboratório de Pesquisa LabPortos, e contou com a colaboração da Coalizão Portuária, da Associação Brasileira das Entidades Portuárias e Hidroviárias (ABEPH) e de um grupo de profissionais especializados nessa temática.

A Coalizão Empresarial Portuária é formada pelas seguintes instituições: Associação de Terminais Portuários Privados (ATP), Associação Brasileira de Terminais de Contêineres (ABRATEC), Associação Brasileira de Terminais de Líquidos (ABTL), Associação Brasileira dos Terminais Portuários (ABTP), Associação Brasileira de Terminais e Recintos Alfandegados (ABTRA) e Federação Nacional das Operações Portuárias (FENOP).

O crescimento do comércio internacional e a complexidade crescente das cadeias logísticas ampliam a exposição das infraestruturas portuárias a diversos de riscos, sejam eles de natureza física, operacional, tecnológica ou jurídica. Nesse cenário, torna-se essencial que terminais portuários e retroportuários adotem boas práticas de segurança voltadas à prevenção de incidentes, à proteção de ativos e à garantia da fluidez operacional, com base em padrões nacionais e internacionais reconhecidos, tais como o Código Internacional para a Proteção de Navios e Instalações Portuárias (ISPS Code) e as diretrizes da Organização Marítima Internacional (IMO).

Desde o início, parte-se do pressuposto de que todas as legislações e regulamentações aplicáveis já são cumpridas pelas organizações. Assim, as práticas aqui sugeridas não substituem obrigações legais, mas se apresentam como estratégias complementares, orientadas ao aprimoramento contínuo da segurança e ao fortalecimento institucional.

É fundamental distinguir os requisitos legais obrigatórios das boas práticas recomendadas. Enquanto a legislação estabelece um padrão mínimo de conformidade, este guia propõe medidas que vão além do cumprimento legal, promovendo níveis superiores de proteção e eficiência operacional. Sua aplicação deve considerar a realidade de cada instalação, levando em conta sua estrutura física, perfil operacional, recursos disponíveis e contexto logístico.

Trata-se, portanto, de recomendações de caráter discricionário, cuja adoção é facultativa e não possui natureza mandatória, devendo ser implementadas conforme a conveniência e viabilidade de cada terminal.

Essas orientações não substituem as normas legais vigentes, nem devem ser interpretadas como obrigações impostas, mas como referenciais de excelência que podem contribuir para o fortalecimento da cultura de segurança e para o alinhamento com padrões internacionais.

Dito isso, para uma aplicação adequada, é imprescindível compreender a diferença entre os escopos de atuação da segurança portuária e da segurança aduaneira, pois, embora complementares, tratam de dimensões distintas do sistema de proteção.

A segurança portuária, nos termos do ISPS Code, aprovado pela Organização Marítima Internacional e incorporado ao ordenamento jurídico brasileiro por meio do Decreto nº 6.411, de 2008, tem por finalidade prevenir e reprimir atos ilícitos que possam comprometer a proteção de navios, instalações portuárias e cargas utilizadas no comércio internacional. Seu foco é a identificação e mitigação de ameaças como terrorismo, sabotagem, tráfico internacional de drogas e outras atividades criminosas que possam afetar a integridade das operações portuárias.

Essa política é implementada no Brasil pela Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Conportos), criada pelo Decreto nº 9.861, de 2019, órgão colegiado e deliberativo vinculado ao Ministério da Justiça e Segurança Pública, responsável por definir diretrizes e procedimentos para a segurança nas áreas portuárias.

Já a segurança aduaneira tem por objetivo assegurar a integridade da cadeia logística internacional e garantir o cumprimento da legislação aduaneira, mediante medidas que promovam o controle de mercadorias, a fluidez do fluxo aduaneiro e a prevenção de ilícitos, como contrabando, descaminho, fraude documental, tráfico de entorpecentes e evasão de tributos.

Sua disciplina normativa está prevista em instrumentos como o Decreto nº 6.759, de 2009 (Regulamento Aduaneiro) e, de modo mais específico, na Portaria RFB nº 143, de 2022, que dispõe sobre o alfandegamento de recintos e os requisitos de segurança aplicáveis.

De acordo com o artigo 40, da Portaria RFB nº 143/2022[1], compete ao titular da unidade da Receita Federal com jurisdição sobre o local ou recinto estabelecer as rotinas operacionais necessárias ao controle e à segurança aduaneira, assegurando o cumprimento rigoroso das normas. As áreas alfandegadas, portanto, estão submetidas a um regime jurídico específico, com padrões de segurança próprios e vinculantes, estabelecidos pela Secretaria Especial da Receita Federal do Brasil. Assim, nem toda prática recomendada em segurança portuária poderá ser automaticamente adotada nesses locais, pois, em muitos casos, já possui caráter obrigatório no âmbito aduaneiro.

[1] "CAPÍTULO V DA GESTÃO E MONITORAMENTO DO LOCAL OU RECINTO, Seção I Da Gestão do Alfandegamento.
Art. 40. Compete ao titular da Unidade da RFB de jurisdição do local ou recinto:
I - estabelecer rotinas operacionais necessárias ao controle e à segurança aduaneira; [...]" (Receita Federal, 2022).

É fundamental, portanto, que cada operador compreenda as obrigações legais que se aplicam à sua realidade, distinguindo-as das boas práticas de caráter voluntário.

O regime internacional de segurança para a navegação e as instalações portuárias, instituído pela Organização Marítima Internacional (IMO) e implementado no Brasil desde julho de 2004, por meio do Código ISPS, detalha os requisitos obrigatórios para governos, autoridades portuárias, empresas de navegação e instalações, e fornece diretrizes para sua implementação.

Esse sistema é complementado por políticas nacionais de segurança pública e aduaneira, coordenadas por órgãos como a Polícia Federal, a Marinha do Brasil e a Receita Federal do Brasil, atuando de forma integrada e cooperativa.

A gestão da segurança deve ser multidisciplinar e colaborativa, envolvendo atores públicos e privados. A criação de comitês de segurança, fóruns de governança e mecanismos de comunicação contínua entre os diferentes stakeholders é uma prática recomendada para garantir alinhamento de ações, resposta rápida a incidentes e compartilhamento de informações.

Além disso, a adoção de tecnologias avançadas, como sistemas de monitoramento inteligente, análise de dados, inteligência artificial e treinamentos regulares, contribui para a prevenção de riscos e o aprimoramento da capacidade operacional.

A construção de uma cultura de segurança que envolva todos os colaboradores é elemento central para a eficácia dessas medidas. A formação contínua, a conscientização sobre riscos e a discussão ativa sobre segurança promovem um ambiente mais resiliente e confiável.

O conteúdo deste guia foi estruturado com base na metodologia SWOT (análise de forças, fraquezas, oportunidades e ameaças), de modo a padronizar a avaliação e oferecer uma orientação estratégica aos gestores, permitindo a identificação dos pontos críticos e das potencialidades de cada instalação, para a definição de ações direcionadas e sustentáveis.

Em síntese, este guia propõe-se a ser uma ferramenta de referência complementar, que não substitui a legislação vigente, mas fortalece a capacidade institucional, estimula a colaboração entre os stakeholders e promove a adoção de boas práticas alinhadas às normas nacionais e internacionais.

O foco é a proteção dos ativos, a integridade das operações e a construção de um ambiente de negócios seguro, previsível e confiável, em consonância com os princípios da segurança portuária e da segurança aduaneira.

Encerrada a apresentação dos fundamentos, objetivos e contexto de aplicação deste Guia de Segurança, torna-se necessário estabelecer o caminho metodológico que orientará a sua implementação prática. Assim, o capítulo seguinte apresenta a metodologia adotada para a construção e aplicação das diretrizes aqui propostas, detalhando os procedimentos, critérios de análise e etapas utilizadas para a identificação de riscos, avaliação das condições operacionais e definição das medidas de prevenção e controle. Essa abordagem metodológica busca assegurar rigor técnico, consistência analítica e aplicabilidade das recomendações ao contexto das operações portuárias e aduaneiras.

2- Metodologia

A elaboração do Guia de Boas Práticas em Segurança Portuária e Aduaneira apoiou-se em uma metodologia sistematizada, orientada pelo referencial da análise SWOT (forças, fraquezas, oportunidades e ameaças), instrumento amplamente utilizado em avaliações institucionais e diagnósticos estratégicos.
O escopo do presente guia contempla os terminais portuários e retroportuários, com ênfase nas dimensões da segurança portuária, conforme os preceitos do Código Internacional para a Proteção de Navios e Instalações Portuárias (ISPS Code), e da segurança da área alfandegada conforme definido na Portaria 143/2022 da Receita Federal.

Para fins de precisão técnica e aderência normativa, cada subcapítulo foi organizado conforme o tipo de segurança tratada – portuária ou aduaneira –considerando que determinadas medidas possuem aplicação específica, enquanto outras apresentam caráter transversal.

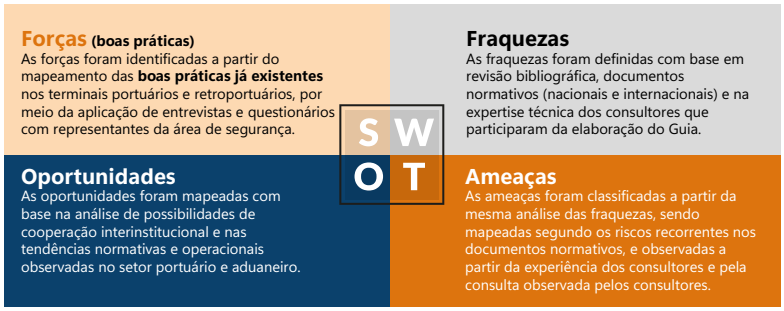
Ressalte-se que, ao longo de todo o guia, a expressão "segurança portuária" refere-se à segurança física como um sistema de prevenção e repressão a atos ilícitos nos portos, terminais e vias navegáveis com vias a contribuir para a proteção do comércio marítimo internacional, proteção das instalações, das cargas e dos acessos, no âmbito das exigências do ISPS Code e da legislação nacional correlata. Não se trata, portanto, de segurança do trabalho, tampouco de segurança operacional no sentido técnico-ocupacional.

Optamos por não adotar a expressão "segurança patrimonial" de forma isolada, uma vez que a segurança aduaneira também compreende, em alguma medida, a proteção patrimonial no contexto do controle de cargas e da prevenção de ilícitos. Assim, a terminologia adotada busca preservar a clareza conceitual, sem prejuízo da delimitação normativa de cada tipo de segurança.

Dessa forma, a estrutura metodológica foi dividida em 4 eixos centrais,

conforme os critérios descritos a seguir, segmentando, sempre que necessário, as boas práticas aplicadas apenas à segurança portuária, apenas à segurança aduaneira ou a ambos.

Figura 1 - Análise SWOT



Fonte: Autoria própria (2026).

Mapeamento das Fraquezas e Ameaças

A primeira etapa consistiu na identificação dos principais riscos e vulnerabilidades que incidem sobre as operações portuárias e retroportuárias. Para tanto, foram utilizados os seguintes instrumentos metodológicos: pesquisa bibliográfica, análise documental, visita técnica nas instalações, exame de normas nacionais e internacionais, pesquisa por meio de formulários eletrônicos, além da contribuição técnica de especialistas e consultores com comprovada experiência na área.

Sabe-se que, na análise SWOT, fraquezas e ameaças não se confundem, possuindo naturezas distintas. As fraquezas dizem respeito a fatores internos da organização, ou seja, pontos em que a própria empresa apresenta limitações. Justamente por serem internas, as fraquezas podem ser trabalhadas e superadas pela própria organização, seja por meio de investimentos, capacitação, reestruturações ou adoção de novas estratégias.

Já as ameaças estão ligadas ao ambiente externo e independem do controle da organização. Embora não possam ser eliminadas pela empresa, as ameaças podem ser monitoradas e enfrentadas com planejamento e adaptação estratégica.

Neste guia, optamos por reunir fraquezas e ameaças em um mesmo capítulo, uma vez que ambos representam aspectos negativos que podem impactar a organização e que, muitas vezes, são analisados em conjunto durante a formulação de estratégias. No entanto, ainda que tratados no mesmo capítulo, cada situação identificada é apresentada em seu respectivo subcapítulo, no qual indicamos de forma precisa se se trata de uma fraqueza ou de uma ameaça. Dessa maneira, garantimos clareza na análise e facilitamos a formulação de estratégias que considerem tanto as vulnerabilidades internas quanto os riscos externos.

As fraquezas e ameaças foram sistematizadas em sete categorias temáticas, consideradas representativas das ocorrências mais sensíveis no setor:

1	2	3	4	5
Terrorismo e sabotagem	Passageiros clandestinos	Roubo, Furto de Carga e Extorsão	Tráfico, Descaminho e Contrabando	Espionagem Industrial
6	**7**			
Treinamento inadequado	Ciberataque			

Este capítulo inicial tem caráter diagnóstico e busca subsidiar os gestores na identificação e na análise dos riscos presentes em suas respectivas infraestruturas.

Levantamento das Boas Práticas e Identificação das Forças Setoriais

Na análise SWOT, as forças representam os aspectos internos positivos da organização, ou seja, os recursos, competências e diferenciais que contribuem para o seu bom desempenho e que a colocam em posição de vantagem frente aos desafios do ambiente.

Nesse sentido, as boas práticas apresentadas neste guia são consideradas as forças dos terminais, pois refletem iniciativas positivas já implementadas e identificadas a partir das entrevistas realizadas com gestores, operadores e consultores do guia.

Essas práticas não se confundem com o cumprimento das obrigações legais ou regulatórias. São ações que vão além do que está previsto em normas e legislações, revelando um esforço voluntário de inovação, aprimoramento contínuo e busca por maior eficiência, segurança e sustentabilidade.

Para estruturar a análise de forma mais clara e prática, as boas práticas foram então correlacionadas às fraquezas e ameaças previamente mapeadas, de modo a demonstrar, de forma objetiva, as estratégias mitigatórias já em operação nos terminais. Essa correlação permite compreender como cada ação contribui diretamente para reduzir vulnerabilidades internas e enfrentar riscos externos, transformando potenciais problemas em oportunidades de fortalecimento.

Assim, este capítulo cumpre a função de valorizar e difundir experiências bem-sucedidas, além de oferecer um panorama das estratégias que já vêm sendo aplicadas pelo setor. Ao reunir essas práticas, o guia fornece subsídios para que outros terminais possam se inspirar e adotar medidas semelhantes, promovendo uma cultura de aprendizado coletivo e elevação dos padrões de desempenho.

Identificação de Oportunidades de Cooperação

As oportunidades correspondem a fatores externos que podem favorecer a organização, isto é, condições, tendências ou iniciativas do ambiente que, se bem aproveitadas, contribuem para fortalecer a atuação, expandir resultados ou melhorar a competitividade. Diferentemente das forças, que são internas, as oportunidades surgem de movimentos do mercado, de políticas públicas, de avanços tecnológicos ou de parcerias estratégicas que criam um cenário favorável para o crescimento e a inovação.

No contexto desse Guia, foram identificadas as seguintes oportunidades que podem ser exploradas para aprimorar os mecanismos de segurança: Cooperação Interagências; Cooperação entre o Público e o Privado; e Políticas Públicas e Financiamento.

Assim, o capítulo de oportunidades evidencia como o ambiente externo pode ser favorável ao avanço da segurança portuária, desde que os atores do setor estejam atentos e preparados para aproveitar esses vetores de fortalecimento. Ao reconhecer e explorar tais oportunidades, é possível transformar potenciais vantagens em resultados concretos para a eficiência e a resiliência dos terminais.

Etapas metodológicas

A partir da delimitação das forças, fraquezas, oportunidades e ameaças que envolvem a segurança portuária e aduaneira no contexto dos terminais portuários e retroportuários, delinearam-se as etapas metodológicas adotadas para a construção desse Guia. A elaboração do conteúdo seguiu um processo estruturado e progressivo, composto por:

Figura 2 - Processo de elaboração do Guia

Fonte: Autoria própria (2026).

1 **Revisão Bibliográfica:** Pesquisa e análise de artigos científicos especializados, nacionais e internacionais, relacionadas à segurança portuária e aduaneira.

2 **Análise de Regulamentações e Normas:** Estudo das principais legislações e normas vigentes, nacionais e internacionais, com destaque para o ISPS Code, Resoluções da Receita Federal, ANTAQ e demais dispositivos legais aplicáveis ao setor.

3 **Entrevistas Presenciais e Remotas:** Realização de entrevistas com gestores de segurança, operadores portuários, autoridades e especialistas indicados pelas organizações, participantes da construção desse Guia. O objetivo foi coletar informações sobre as melhores práticas.

4 **Aplicação de Questionário:** Utilização de instrumento estruturado para coleta de dados com lideranças indicadas pelas organizações, atuantes em diferentes portos e terminais, abordando temas como: terrorismo, roubo de cargas, extorsão, tráfico,

passageiros clandestinos, espionagem econômica e segurança cibernética. O objetivo foi ter uma nova rodada de coleta de melhores práticas do mercado.

5 **Visitas Técnicas:** Investigação *in loco* em instalações portuárias e retroportuárias selecionadas pelas organizações, para observação direta das práticas de segurança e dos sistemas de controle implementados.

6 **Mapeamento e Categorização das Melhores Práticas:** Organização e classificação das práticas identificadas, segundo três eixos: segurança portuária, segurança aduaneira e segurança integrada, aplicando técnicas de análise de conteúdo.

7 **Validação:** Discussão e consolidação dos achados com os consultores da equipe técnica do Guia, membros das organizações participantes desse Guia e seus respectivos comitês de segurança.

8 **Elaboração das Diretrizes:** Síntese estruturada das informações coletadas, traduzida em um conjunto de recomendações práticas voltadas à ampliação da segurança portuária e aduaneira no Brasil.

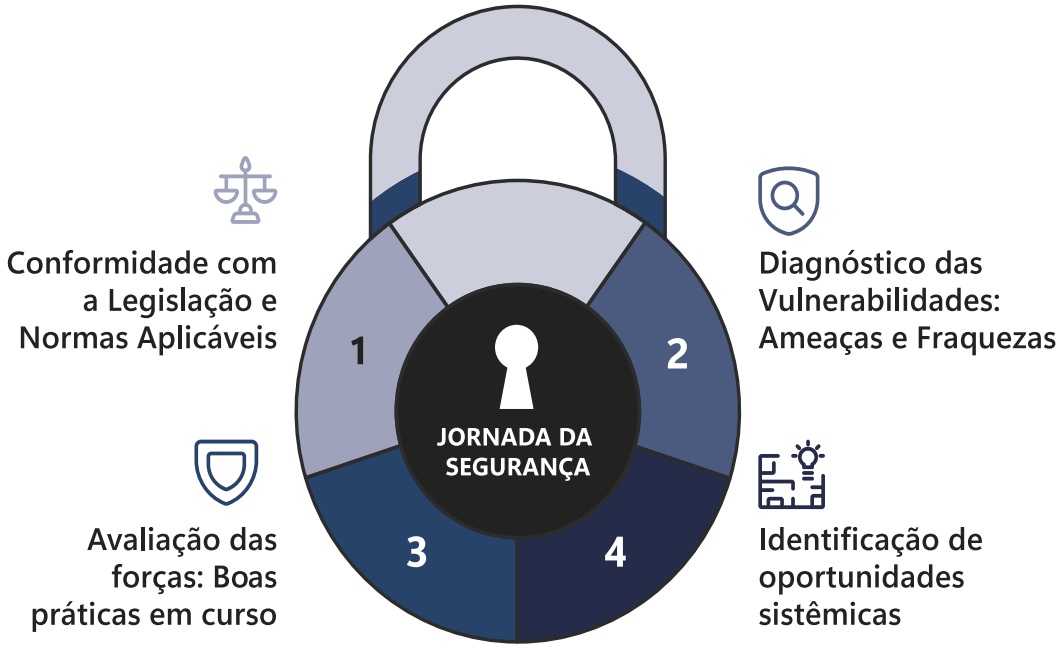
Concluída a apresentação da metodologia utilizada para a análise e estruturação deste Guia de Segurança, torna-se possível avançar para a etapa de consolidação das orientações práticas decorrentes desse processo. Dessa forma, o próximo capítulo apresenta as diretrizes de segurança que orientam a prevenção de riscos, a organização das rotinas operacionais e a adoção de boas práticas no ambiente portuário e logístico. Essas diretrizes traduzem, em recomendações objetivas, os resultados obtidos a partir da metodologia aplicada, buscando contribuir para a melhoria contínua das condições de segurança nas operações.

3- Diretrizes para a aplicação do guia

Esse capítulo tem por finalidade estabelecer diretrizes objetivas para a adequada utilização do Guia de Boas Práticas em Segurança Portuária e Aduaneira, instrumento que visa a fortalecer a gestão da segurança em instalações portuárias e retroportuárias.

O fluxograma a seguir, de caráter ilustrativo, apresenta as etapas propostas para a aplicação estruturada do Guia:

Figura 3 - Etapas propostas para a aplicação estruturada do Guia



Fonte: Autoria própria (2026).

ETAPA 1 | Conformidade com a Legislação e Normas Aplicáveis

Antes da adoção de qualquer recomendação contida neste Guia, a instalação portuária ou recinto alfandegado deverá assegurar o integral cumprimento das normas legais, regulamentares e infralegais vigentes, as quais constituem o alicerce da segurança

portuária e aduaneira.

Ressalta-se que o Guia parte do pressuposto de que o terminal já observa todos os requisitos normativos mínimos exigidos pelas autoridades competentes.

As principais normas de referência estão consolidadas no Capítulo 4, sem prejuízo de outras que venham a ser aplicáveis em razão da natureza específica da operação ou da jurisdição regulatória. O Guia, portanto, não substitui os marcos legais, mas atua de forma complementar, orientando a adoção de boas práticas com base na experiência técnica consolidada no setor.

ETAPA 2 Diagnóstico das Vulnerabilidades: Ameaças e Fraquezas

Com base na matriz SWOT (Forças, Fraquezas, Oportunidades e Ameaças), o terminal deverá realizar uma autoavaliação das suas vulnerabilidades. Para tanto, o Capítulo 7 apresenta um conjunto de ameaças externas e fraquezas internas, que afetam com frequência as instalações portuárias e retroportuárias.

Esses elementos foram definidos a partir de revisão bibliográfica, análise documental de normas nacionais e internacionais, bem como da expertise técnica dos profissionais envolvidos na elaboração do Guia. Compete à instalação, com base nesse referencial, identificar quais riscos efetivamente se aplicam à sua realidade operacional, de modo a construir seu próprio diagnóstico estratégico.

Importa destacar, contudo, que o presente Guia não tem por objetivo esgotar ou abarcar a totalidade dos riscos possíveis. Por razões metodológicas e de escopo, foi necessário delimitar o rol de ameaças

e fraquezas abordadas, priorizando aquelas com maior incidência ou potencial lesivo, conforme as evidências obtidas.

Dessa forma, a instalação não deve restringir sua análise exclusivamente aos riscos descritos no Capítulo 7. É recomendável que o terminal complemente sua matriz SWOT com informações adicionais advindas de diagnósticos internos, auditorias anteriores, análises de risco específicas ou outros documentos estratégicos, adaptando a aplicação do Guia à sua realidade operacional e ao seu grau de exposição a diferentes vetores de ameaça.

ETAPA 3 | Avaliação das Forças: Boas Práticas em Curso

O Capítulo 8 do Guia elenca as boas práticas atualmente implementadas por diversos terminais portuários e retroportuários, as quais são aqui tratadas como "forças", no sentido da metodologia SWOT. A coleta dessas práticas deu-se por meio de entrevistas presenciais, formulários e contribuições técnicas colhidas junto a profissionais da área, refletindo experiências positivas em vigor no setor.

Cada força apresentada está correlacionada diretamente a uma ou mais ameaças e fraquezas destacadas no Capítulo 7, permitindo ao terminal estabelecer uma resposta concreta e adequada aos riscos previamente identificados. Recomenda-se que a instalação avalie se tais práticas já se encontram implementadas, se podem ser aprimoradas ou se devem ser incorporadas, considerando sua viabilidade, relevância e aderência ao contexto local.

ETAPA 4 | Identificação de Oportunidades Sistêmicas

Por fim, o Capítulo 9 trata das oportunidades, entendidas como possibilidades de fortalecimento da segurança a partir da articulação entre diferentes agentes – públicos e privados – que atuam no ambiente portuário e alfandegado. Tais oportunidades incluem, por

exemplo, iniciativas de cooperação interinstitucional, desenvolvimento de protocolos integrados e compartilhamento de informações.

Ao contrário das forças, que dependem de ações internas, as oportunidades exigem articulação externa e, muitas vezes, intervenção normativa ou institucional. Ainda assim, sua identificação e análise são relevantes para o planejamento estratégico do terminal, podendo subsidiar pleitos, parcerias e projetos de melhoria contínua.

Após a apresentação das diretrizes que orientam a adoção de boas práticas e o fortalecimento das rotinas de prevenção e controle no ambiente portuário, torna-se fundamental compreender o arcabouço jurídico que sustenta essas ações. Nesse sentido, o capítulo seguinte apresenta a legislação aplicável à segurança portuária e aduaneira, reunindo os principais dispositivos normativos que estabelecem competências institucionais, requisitos operacionais e instrumentos regulatórios que orientam a atuação dos diversos órgãos envolvidos na proteção das infraestruturas portuárias e das operações de comércio exterior.

4- Legislação aplicada

A atuação dos terminais portuários e retroportuários no campo da segurança portuária e aduaneira está submetida a um complexo arcabouço jurídico estruturado em diferentes níveis normativos, que abrange normas constitucionais, legislação infraconstitucional, tratados internacionais incorporados ao ordenamento jurídico brasileiro, além de atos normativos expedidos por órgãos da Administração Pública direta e indireta, no exercício de suas competências regulatórias e fiscalizatórias.

O marco inicial desse sistema encontra-se na Constituição Federal de 1988, cujo artigo 144 define que a segurança pública é dever do Estado, direito e responsabilidade de todos, sendo exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio.

A partir desse fundamento constitucional, foram instituídas normas infraconstitucionais que detalham e operacionalizam os mecanismos de prevenção, repressão e investigação de ilícitos, inclusive no âmbito das infraestruturas críticas e portuárias.

A aplicação das boas práticas aqui apresentadas deve considerar a realidade operacional de cada instalação, levando em conta fatores como perfil de carga, porte do terminal, recursos tecnológicos disponíveis e localização geográfica, de modo a garantir proporcionalidade e efetividade na adoção das medidas.

Assim, cabe a cada operador avaliar, com base em critérios técnicos e na gestão de riscos, quais práticas são aplicáveis e em que grau podem ser adotadas, respeitando sempre os limites da razoabilidade e da proporcionalidade.

Para fins de referência, as normas aplicáveis ao tema são elencadas a seguir, organizadas em ordem decrescente de hierarquia normativa, conforme os princípios que regem a estrutura do ordenamento jurídico brasileiro. Essa ordenação tem por objetivo conferir clareza quanto à autoridade e ao alcance de cada norma, facilitando a sua correta interpretação e aplicação.

4.1 SEGURANÇA PORTUÁRIA

The International Maritime Dangerous Goods (IMDG) Code, 1965

Órgão:	N/A
Ementa:	O Código IMDG (International Maritime Dangerous Goods Code), publicado pela primeira vez em 1965 pela Organização Marítima Internacional (IMO), estabelece normas internacionais para o transporte seguro de cargas perigosas por via marítima. A partir de 1º de janeiro de 2004, o código passou a ter aplicação obrigatória sob a Convenção SOLAS, embora algumas disposições ainda permaneçam recomendatórias.

ISPS Code – International Ship and Port Facility Security Code de julho de 2004

Órgão:	IMO
Ementa:	A Conferência Diplomática sobre Segurança Marítima realizada em Londres, em dezembro de 2002, adotou novas disposições na Convenção Internacional para a Salvaguarda da Vida Humana no Mar de 1974, com vistas a intensificar a proteção marítima. Esses novos requisitos formam a estrutura internacional por meio da qual navios e instalações portuárias podem cooperar para detectar e dissuadir atos que ameacem a proteção no setor de transporte marítimo.

Decreto nº 6.869, de 4 de junho de 2009

Órgão:	Presidência da República
Ementa:	Dispõe sobre a coordenação e articulação dos órgãos federais, bem como sobre os níveis de proteção dos navios e das instalações portuárias, da adoção de medidas de proteção aos navios e instalações portuárias, e institui a Rede de Alarme e Controle dos Níveis de Proteção de Navios e Instalações Portuárias, e dá outras providências.

Lei nº 12.815, de 5 de junho de 2013 – Exploração dos Portos

Órgão:	Presidência da República
Ementa:	Dispõe sobre a exploração direta e indireta pela União de portos e instalações portuárias e sobre as atividades desempenhadas pelos operadores portuários.

Decreto nº 8.033, de 27 de junho de 2013 – Regulamentação da Lei dos Portos

Órgão:	Presidência da República
Ementa:	Regulamenta o disposto na Lei nº 12.815, de 5 de junho de 2013, e as demais disposições legais que regulam a exploração de portos organizados e de instalações portuárias.

Decreto nº 9.861, de 25 de junho de 2019

Órgão:	Presidência da República
Ementa:	Dispõe sobre a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis e sobre as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis.

Decreto nº 9.988, de 26 de agosto de 2019 e Anexos SOLAS

Órgão:	Presidência da República
Ementa:	Promulga o texto atualizado da Convenção Internacional para a Salvaguarda da Vida Humana no Mar. E promulga os anexos completos da Convenção Internacional para a Salvaguarda da Vida Humana no Mar (SOLAS), que incluem disposições sobre segurança portuária.

Resolução nº 53, de 04 de setembro de 2020

Órgão:	CONPORTOS
Ementa:	Dispõe acerca da consolidação e atualização das Resoluções da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis, conforme normas do Código ISPS.

Resolução Normativa nº 65, de 14 de dezembro de 2021 – Operações com produtos perigosos

Órgão:	ANTAQ
Ementa:	Esta Resolução incorpora aspectos de segurança e saúde ocupacional, preservação da integridade física das instalações portuárias e proteção do meio ambiente oriundos do Código Marítimo Internacional de Mercadorias Perigosas / *International Maritime Dangerous Goods Code* (Código IMDG) e do Código Internacional para a Proteção de Navios e Instalações Portuárias / *International Ship and Port Facility Security Code* (Código ISPS), regulamentos da Organização Marítima Internacional (IMO), bem como se harmoniza com a NR 29 – Norma Regulamentadora de Segurança e Saúde no Trabalho Portuário, do Ministério do Trabalho e Previdência, com a Resolução ANTT nº 5.947, de 1º de junho de 2021, da Agência Nacional de Transportes Terrestres (ANTT), com a Lei nº 9.719, de 27 de novembro de 1998, e com outros regulamentos pertinentes à matéria, que devem ser usados em complemento a essa Resolução no que couber e não conflitar.

Resolução Normativa nº 71, de 30 de março de 2022 – Exploração de TUP

Órgão:	ANTAQ
Ementa:	Estabelece os procedimentos para autorização de construção e exploração de terminal de uso privado, de estação de transbordo de carga, de instalação portuária pública de pequeno porte e de instalação portuária de turismo.

Resolução Normativa nº 127, de 08 de abril de 2025 – Exploração de áreas sob gestão da Administração Portuária

Órgão:	ANTAQ
Ementa:	Regulamenta a exploração de áreas e instalações portuárias delimitadas pela poligonal do porto organizado.

4.2 SEGURANÇA ADUANEIRA

Decreto-Lei nº 37, de 18 de novembro de 1966

Órgão:	Presidência da República
Ementa:	Dispõe sobre o imposto de importação, reorganiza os serviços aduaneiros e dá outras providências, *como Controle Aduaneiro, Jurisdição dos Serviços Aduaneiros.*

Decreto nº 660, de 25 de setembro de 1992

Órgão:	Presidência da República
Ementa:	Institui o Sistema Integrado de Comércio Exterior (SISCOMEX).

Instrução Normativa RFB n.º 248, de 25 de novembro de 2002

Órgão:	Receita Federal
Ementa:	Dispõe sobre a aplicação do regime de trânsito aduaneiro.

Instrução Normativa RFB nº 680, de 2 de outubro de 2006

Órgão:	Receita Federal do Brasil
Ementa:	Dispõe sobre os procedimentos de controle aduaneiro na importação.

Decreto nº 6.759, de 5 de fevereiro de 2009 – Regulamento Aduaneiro

Órgão:	Presidência da República
Ementa:	Regulamenta a administração das atividades aduaneiras e a fiscalização, controle e tributação das operações de comércio exterior.

Instrução Normativa RFB nº 1.702, de 21 de março de 2017

Órgão:	Receita Federal do Brasil
Ementa:	Disciplina o despacho aduaneiro de exportação processado por meio de Declaração Única de Exportação (DU-E).

Tratado Internacional - Acordo de Facilitação do Comércio da OMC de dezembro de 2013 e Decreto n.º 9.326, de 3 abril de 2018

Órgão:	Organização Mundial do Comércio – OMC e Presidência da República
Ementa:	O Acordo de Facilitação de Comércio foi adotado na IX Conferência Ministerial da Organização Mundial do Comércio, realizada em Bali, Indonésia, em dezembro de 2013. O Acordo contempla medidas para modernizar a administração aduaneira e simplificar e agilizar os procedimentos de comércio exterior, além de possibilitar a cooperação entre os Membros na prevenção e combate a delitos aduaneiros. Promulgado e Adotado pelos Membros da OMC, e internalizado pelo BR por meio do Decreto n.º 9.326, de 3 de abril de 2018.

Portaria RFB nº 143, de 11 de fevereiro de 2022

Órgão:	Receita Federal do Brasil
Ementa:	Estabelece normas gerais e procedimentos para o alfandegamento de local ou recinto.

Portaria Coana nº 72, de 12 de abril de 2022 (multivigente com posteriores alterações, incluindo a Portaria Coana n.º 138, de 14 de setembro de 2023)

Órgão:	Coordenação-Geral de Administração Aduaneira da Receita Federal do Brasil – Coana
Ementa:	Especifica os requisitos técnicos, formais e de segurança para registro e armazenamento de informações em sistema informatizado de controle aduaneiro (SICA) e o envio de eventos à *Application Programming Interface* Recintos (API-Recintos) do Portal Único de Comércio Exterior no Sistema Integrado de Comércio Exterior (Portal Siscomex), pelos intervenientes que operam em locais ou recintos alfandegados ou autorizados a operar com mercadorias, sob controle aduaneiro.

Portaria Conjunta Coana / Cotec nº 74, de 11 de maio de 2022

Órgão:	Coordenação-Geral de Administração Aduaneira da Receita Federal do Brasil - Coana e Coordenação Geral de Tecnologia e Segurança da Informação- Cotec
Ementa:	Dispõe sobre normas, especificações e procedimentos para a implantação de infraestrutura de tecnologia da informação e comunicação e de mobiliário nas áreas de atuação da Secretaria Especial da Receita Federal do Brasil (RFB), em local ou recinto alfandegado.

Portaria Coana nº 75, de 12 de maio de 2022 (multivigente com posteriores alterações, incluindo a Portaria Coana n.º 132, de 31 de julho de 2023)

Órgão:	Coordenação-Geral de Administração Aduaneira da Receita Federal do Brasil – Coana
Ementa:	Regulamenta os requisitos e procedimentos para a verificação física e remota de mercadorias, a verificação de mercadorias pelo importador, a verificação remota de cargas submetidas ao trânsito aduaneiro e as especificações técnicas e requisitos mínimos do respectivo sistema informatizado.

Portaria Coana nº 76, de 13 de maio de 2022 (multivigente com posteriores alterações, incluindo a Portaria Coana n.º 144, de 27 de novembro de 2023)

Órgão:	Coordenação-Geral de Administração Aduaneira da Receita Federal do Brasil – Coana
Ementa:	Dispõe sobre as especificações técnicas e as condições relativas às áreas segregadas de escritórios e alojamentos, aos instrumentos e aparelhos de inspeção não invasiva, à dispensa de submissão a mais de uma inspeção não invasiva de contêineres movimentados em trânsito aduaneiro, ao compartilhamento de equipamentos e sistemas; aprova os modelos de Ato Declaratório Executivo para o alfandegamento e o desalfandegamento, de termo de fiel depositário e de designação de preposto e disciplina o tratamento prioritário a ser dispensado às cargas do Operador Econômico Autorizado.

Portaria Coana nº 80, de 23 de junho de 2022 (multivigente com posteriores alterações, incluindo a Portaria Coana n.º 132, de 31 de julho de 2023)

Órgão:	Coordenação-Geral de Administração Aduaneira da Receita Federal do Brasil – Coana
Ementa:	Especifica as condições de funcionamento e os requisitos técnicos mínimos do sistema de monitoramento e vigilância de local ou recinto alfandegado e suas funcionalidades.

Instrução Normativa RFB nº 2154, de 26 de julho de 2023 (multivigente com posterior alteração pela Instrução Normativa RFB n.º 2200, de 12 de julho de 2024)

Órgão:	Receita Federal do Brasil
Ementa:	Dispõe sobre o Programa Brasileiro de Operador Econômico Autorizado.

Instrução Normativa nº 2.169, de 29 de dezembro de 2023

Órgão:	Receita Federal
Ementa:	Aprova o texto consolidado das Notas Explicativas do Sistema Harmonizado de Designação e de Codificação de Mercadorias publicadas pela Organização Mundial das Alfândegas (OMA).

Instrução Normativa RFB nº 2.171, de 2 de janeiro de 2024

Órgão:	Receita Federal
Ementa:	Aprova a Coletânea dos pareceres de classificação do Comitê do Sistema Harmonizado da Organização Mundial das Alfândegas (OMA).

Portaria RFB nº 435, de 02 de julho de 2024

Órgão:	Receita Federal do Brasil
Ementa:	Dispõe sobre a participação de órgãos e entidades da administração pública no Programa Brasileiro de Operador Econômico Autorizado, por intermédio de módulo complementar do OEA-Integrado.

Apresentado o conjunto de normas que compõem o marco regulatório da segurança portuária e aduaneira, torna-se necessário compreender como essas disposições legais se traduzem na prática institucional. Nesse contexto, o próximo capítulo apresenta as atribuições dos diferentes órgãos e entidades envolvidos na segurança portuária e aduaneira, detalhando responsabilidades, competências e formas de atuação que estruturam o sistema de proteção das instalações portuárias e das operações de comércio exterior.

5- Atribuições na segurança portuária e aduaneira

A segurança portuária brasileira está fundada em um arcabouço jurídico robusto que define de forma clara as atribuições legais e institucionais dos órgãos públicos responsáveis pela prevenção e repressão de ilícitos nas áreas portuárias, terminais e vias navegáveis. A delimitação precisa dessas competências é condição essencial para uma atuação harmônica, eficaz e juridicamente segura do sistema de proteção dos portos nacionais.

Este capítulo apresenta as atribuições dos principais entes envolvidos na segurança portuária e aduaneira, bem como suas bases legais e a forma como interagem no exercício de suas funções.

5.1 Portuária

5.1.1 Polícia Federal

A Polícia Federal é o órgão central da União no campo da segurança pública federal. Suas atribuições estão expressamente previstas na Constituição Federal, no artigo 144, parágrafo primeiro, e abrangem (i) a apuração de infrações penais de competência da União, (ii) a prevenção e repressão do tráfico ilícito de entorpecentes, do contrabando e do descaminho, (iii) o exercício das funções de polícia judiciária da União e (iv) a atuação como polícia marítima, aeroportuária e de fronteiras (Brasil, 1988).

Cabe à Polícia Federal, portanto, a investigação de crimes de natureza federal, o desenvolvimento das ações de polícia judiciária correspondentes e a preservação da cadeia de custódia dos materiais apreendidos. Além das atribuições constitucionais, a estrutura administrativa da Polícia Federal é regulamentada pelo Decreto nº 11.348, de 2023, que, entretanto, não amplia ou modifica suas competências, servindo apenas para dispor sobre sua organização e funcionamento.

No contexto portuário, a Polícia Federal é responsável pela apuração de ilícitos penais de competência federal, pela coordenação de ações que envolvam crimes como o tráfico de drogas e contrabando e pela preservação do local de crime e da integridade da cadeia de custódia. Assim, quando houver suspeita de crime de natureza federal nas áreas portuárias, a comunicação imediata à Polícia Federal é imprescindível para garantir a legalidade do procedimento e evitar nulidades processuais decorrentes de falhas na preservação de provas.

5.1.2 CONPORTOS e CESPORTOS

A Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS), instituída pelo Decreto nº 9.861/2019, é um órgão colegiado vinculado ao Ministério da Justiça e Segurança Pública, com caráter deliberativo e permanente, tendo como presidente um representante da Polícia Federal. Compete à CONPORTOS estabelecer normas e diretrizes para a segurança portuária; homologar Estudos de Avaliação de Riscos (EAR) e Planos de Segurança Portuária (PSP); bem como supervisionar auditorias e avaliar conformidade com o Código ISPS.

Em âmbito estadual, atuam as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CESPORTOS), compostas, exclusivamente, por representantes da Polícia Federal, Capitania dos Portos, da Secretaria Especial da Receita Federal do Brasil, da Agência Nacional de Transportes Aquaviários (ANTAQ), das Unidades de Segurança das Administrações Portuárias e das Secretarias Estaduais de Segurança Pública. A participação de outros órgãos e entidades é excepcional, admitida apenas na condição de convidados e sem direito a voto, quando a natureza da matéria justificar.

O Código ISPS, elaborado pela Organização Marítima Internacional,

após os atentados de 11 de setembro de 2001, estabelece padrões internacionais de segurança marítima e portuária, visando a prevenir ameaças como o terrorismo, o tráfico de drogas e o contrabando. No Brasil, sua aplicação é garantida por meio da Declaração de Cumprimento, documento que certifica que a instalação portuária atende aos requisitos do Código, às disposições da Convenção SOLAS e às resoluções da Conportos. Para a obtenção dessa certificação, a instalação deve apresentar um Estudo de Avaliação de Risco à Cesportos, que o analisa e o encaminha à Conportos para homologação. Em seguida, deve elaborar um Plano de Segurança Portuária com as medidas mitigatórias apontadas, submetendo-o a nova análise e a uma inspeção in loco. O artigo 72, do Decreto nº 9.861/2019, estabelece que a Cesportos deve realizar a inspeção no prazo máximo de noventa dias, indicando eventuais ajustes antes da homologação pela Conportos.

As auditorias realizadas pela Conportos têm como objetivo verificar se as atividades de segurança das instalações portuárias estão em conformidade com os estudos e planos aprovados, bem como avaliar a efetividade e a eficiência dos sistemas e procedimentos implementados. Essas auditorias são programadas a cada cinco anos, sem prejuízo de outras inspeções que possam ser determinadas conforme as circunstâncias.

A metodologia ARESP, desenvolvida pela Conportos, é utilizada para orientar as avaliações de risco e subsidiar a elaboração dos planos de segurança portuária. Essa metodologia considera fatores internos e externos às instalações e avalia o nível de ameaça com base na motivação, capacidade e acessibilidade, abrangendo riscos como o crime organizado, o terrorismo, as ameaças cibernéticas, os desastres e as ameaças internas. A Deliberação Conportos nº 1.104, de 2024, isenta da obrigatoriedade de elaboração do PSP as instalações que não possuam acesso aquaviário ou interface com navios de longo

curso. Ainda assim, a certificação ISPS representa apenas o requisito mínimo de conformidade, não sendo suficiente, por si só, para garantir a segurança plena. A segurança portuária deve ser encarada como um processo contínuo e dinâmico, capaz de se adaptar à evolução constante das ameaças.

5.1.3 Supervisores de Segurança Portuária

A estrutura de segurança portuária também é composta pelos Supervisores de Segurança Portuária, pelos elementos organizacionais internos e pelas Organizações de Segurança (OS). Os Supervisores são profissionais devidamente habilitados pela Conportos, por meio do Curso Especial de Supervisor de Segurança Portuária, com a responsabilidade de implementar e manter as medidas previstas no Código ISPS e nas resoluções da Conportos. As Organizações de Segurança são empresas credenciadas, com capacitação técnica para elaborar os Estudos de Avaliação de Risco (EAR) e os Planos de Segurança Portuária (PSP). Elementos organizacionais constituídos dentro das estruturas administrativas das instalações portuárias, quando exercem essas funções, são equiparados às OS.

5.2 Aduaneira

A Secretaria Especial da Receita Federal do Brasil (RFB) é o órgão responsável pela administração e fiscalização aduaneira no território nacional. Sua atuação compreende o controle das mercadorias, veículos e pessoas que entram e saem do país, em portos, aeroportos, pontos de fronteira e recintos alfandegados, assegurando o cumprimento da legislação aduaneira, aplicando medidas fiscais e restritivas e contribuindo para a segurança pública e nacional. Além disso, colabora com outros órgãos anuentes para a proteção do meio ambiente, da saúde pública e da biossegurança.

A segurança aduaneira tem por objetivo assegurar a integridade da cadeia logística internacional e garantir o cumprimento da

legislação aduaneira, mediante medidas que promovam o controle de mercadorias, a fluidez do fluxo aduaneiro e a prevenção de ilícitos, como contrabando, descaminho, fraude documental, tráfico de entorpecentes e evasão de tributos.

Sua disciplina normativa está prevista no Decreto nº 6.759, de 2009 (Regulamento Aduaneiro), e, de modo mais específico, na Portaria RFB nº 143, de 2022, que dispõe sobre o alfandegamento de recintos e define os requisitos de segurança a serem observados pelos terminais. De acordo com o artigo 40 da referida Portaria, compete ao titular da unidade da Receita Federal com jurisdição sobre o local ou recinto estabelecer as rotinas operacionais necessárias ao controle e à segurança aduaneira, assegurando o cumprimento rigoroso das normas.

O Ato Declaratório Executivo (ADE) de Alfandegamento, emitido com base na Portaria nº 143/2022, constitui o principal instrumento de certificação da segurança aduaneira. Sua concessão atesta que o recinto cumpre todos os requisitos legais, incluindo infraestrutura adequada, sistemas de vigilância e controle de acesso, monitoramento 24 horas, integração com sistemas informatizados e procedimentos de gerenciamento de riscos. O ADE representa, assim, o reconhecimento formal de conformidade e segurança aduaneira, funcionando como um selo institucional que habilita a instalação a operar sob regime alfandegado.

A Portaria RFB nº 143/2022 é complementada por um conjunto de Portarias da Coordenação-Geral de Administração Aduaneira (COANA), que detalham as exigências técnicas e operacionais para o alfandegamento e manutenção dos recintos:

A Portaria COANA nº 72, de 2022, estabelece os requisitos técnicos, formais e de segurança para o registro e armazenamento

de informações em sistema informatizado de controle aduaneiro (SICA), bem como para o envio de eventos à API-Recintos do Portal Único de Comércio Exterior, garantindo a integração e a rastreabilidade das operações.

A Portaria COANA nº 75, de 2022, regulamenta os procedimentos de verificação física e remota de mercadorias, incluindo inspeções aduaneiras e controles realizados por sistemas automatizados, além de definir as especificações técnicas mínimas desses sistemas.

A Portaria COANA nº 76, de 2022, dispõe sobre as condições de infraestrutura física e tecnológica dos recintos, incluindo áreas segregadas, equipamentos de inspeção não invasiva, regras de compartilhamento de recursos e tratamento prioritário às cargas de Operadores Econômicos Autorizados (OEA), além de aprovar os modelos de ADE e termos de fiel depositário.

A Portaria COANA nº 80, de 2022, define os requisitos mínimos dos sistemas de monitoramento e vigilância de recintos alfandegados, estabelecendo padrões de funcionamento contínuo, registro de ocorrências e transmissão em tempo real às unidades da Receita Federal.

Essas normas compõem o conjunto regulatório de segurança aduaneira aplicável aos recintos alfandegados, assegurando que os locais autorizados operem conforme padrões uniformes de controle e integridade, integrados ao Programa do Portal Único de Comércio Exterior, que busca simplificar, harmonizar e tornar previsíveis os fluxos de comércio exterior.

A segurança aduaneira, no contexto da Receita Federal do Brasil, é implementada não apenas por meio das ações de controle e fiscalização previstas na legislação, mas também por instrumentos estratégicos de modernização, como gerenciamento de riscos,

uso intensivo de tecnologia da informação e cooperação com o setor privado. A Instrução Normativa RFB nº 2.154, de 2023, que regulamenta o Programa Operador Econômico Autorizado (OEA), complementa essa política ao promover a segurança e a conformidade da cadeia logística internacional, reconhecendo e certificando intervenientes de baixo risco.

Dessa forma, a segurança aduaneira constitui uma função estratégica e preventiva, que se concretiza por meio das atividades de controle e fiscalização, mas as transcende ao adotar uma visão integrada de proteção e facilitação do comércio exterior, conforme as orientações do SAFE *Framework of Standards*, da Organização Mundial das Aduanas (OMA), do qual o Brasil é signatário.

Após a apresentação das atribuições institucionais relacionadas à segurança portuária e aduaneira, torna-se relevante compreender quem são os agentes que, na prática, integram esse sistema e participam diretamente das atividades de prevenção, controle e resposta a riscos. Dessa forma, o capítulo seguinte apresenta os principais atores envolvidos na segurança do ambiente portuário, destacando o papel de cada instituição e a importância da atuação coordenada entre os diferentes órgãos públicos, operadores e demais participantes da comunidade portuária e aduaneira.

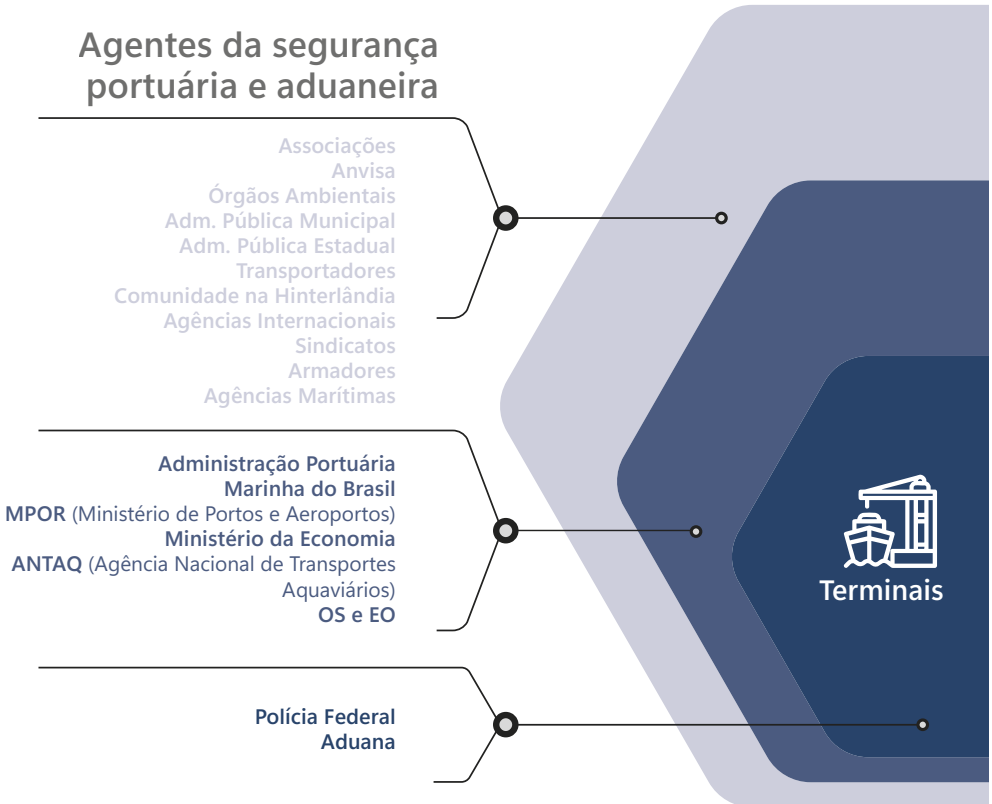
6- Principais atores na segurança portuária e aduaneira

Em um ambiente de crescente complexidade normativa e operacional, os terminais portuários e retroportuários tornaram-se espaços de atuação integrada de diversos órgãos públicos e entes privados, cujas atribuições se entrelaçam na implementação de medidas de controle, prevenção e repressão a ilícitos.

Este capítulo tem por objetivo identificar e analisar os principais atores envolvidos na segurança dos terminais brasileiros, tanto sob a ótica da segurança pública quanto do controle aduaneiro.

A Figura 4 apresenta, de forma esquemática, a estrutura sistêmica da segurança portuária e aduaneira no Brasil, destacando graficamente os principais atores que exercem funções centrais na proteção das instalações portuárias/retroportuárias e no controle das operações de comércio exterior.

Figura 4 - Estrutura sistêmica da segurança portuária e aduaneira no Brasil -



Fonte: Autoria própria (2026).

No núcleo da representação visual, encontram-se os entes com atribuições normativas, fiscalizatórias e operacionais mais relevantes nesse contexto. São os agentes determinantes dentro da segurança portuária e aduaneira.

Distribuídos ao redor do núcleo central, o segundo círculo da Figura 4 contempla os atores secundários, mas de importância estratégica e complementar, cuja atuação reforça e sustenta o sistema de segurança portuária e aduaneira. Ainda que não desempenhem papel primário na definição ou execução das medidas de controle, esses entes exercem funções regulatórias, institucionais e de inteligência que impactam diretamente a eficácia do sistema como um todo.

No terceiro e mais externo círculo, situam-se outros atores que, embora mais periféricos, também desempenham funções relevantes na consolidação de um ambiente seguro e controlado nos terminais. Incluem-se nesse grupo as associações setoriais, como entidades representativas de terminais portuários e retroportuários, que contribuem para a uniformização de boas práticas e o diálogo institucional com os órgãos reguladores e fiscalizadores.

Apresenta-se, a seguir, o detalhamento da formação institucional, competências legais e atribuições práticas dos principais atores que atuam no sistema de segurança portuária e aduaneira, com especial atenção à atuação integrada entre os órgãos de segurança pública, controle aduaneiro, entidades internacionais e operadores portuários.

ANVISA

A Agência Nacional de Vigilância Sanitária (ANVISA), autarquia sob regime especial vinculada ao Ministério da Saúde e instituída pela Lei nº 9.782/1999, é responsável pelo controle sanitário de portos, aeroportos, fronteiras e recintos alfandegados, atuando como órgão

anuente nas operações de comércio exterior e como autoridade sanitária nas instalações portuárias. Compete-lhe fiscalizar produtos e serviços sujeitos à vigilância sanitária, inspecionar embarcações, emitir o Certificado de Livre Prática (CLP) e o Certificado Sanitário de Embarcação – Controle de Saúde de Bordo (Ship Sanitation Certificate, SSC), controlar resíduos e efluentes, e coordenar medidas de biossegurança e resposta a emergências de saúde pública, em conformidade com o Regulamento Sanitário Internacional (RSI/2005). Nos portos, a ANVISA atua de forma integrada com a Receita Federal, Polícia Federal, Marinha do Brasil, MAPA e CONPORTOS/CESPORTOS, prevenindo riscos biológicos, químicos e epidemiológicos e assegurando que as operações de comércio exterior ocorram de modo seguro e compatível com a proteção da saúde pública.

ANTAQ

A Agência Nacional de Transportes Aquaviários (ANTAQ), autarquia sob regime especial vinculada ao Ministério de Portos e Aeroportos, instituída pela Lei nº 10.233/2001, é responsável por regular, supervisionar e fiscalizar as atividades de prestação de serviços de transporte aquaviário e de exploração da infraestrutura portuária e hidroviária, assegurando eficiência, segurança e modicidade tarifária.

No contexto da segurança portuária e aduaneira, a ANTAQ exerce papel estratégico ao estabelecer normas operacionais e técnicas que impactam diretamente o controle de riscos e a integridade das operações, por meio de Resoluções Normativas que disciplinam o funcionamento de terminais públicos e privados, o manuseio de cargas perigosas, a segurança ambiental e as condições de exploração de áreas sob gestão portuária. Atua em cooperação com a CONPORTOS/CESPORTOS, Receita Federal, Marinha do Brasil e Polícia Federal, fiscalizando o cumprimento das normas de segurança e as condições de operação das instalações portuárias, contribuindo para a prevenção de acidentes, ilícitos e ameaças à

integridade física, ambiental e patrimonial do sistema portuário brasileiro.

POLÍCIA FEDERAL

A Polícia Federal (PF), órgão permanente da Administração Pública Federal, integrante do Ministério da Justiça e Segurança Pública e prevista no artigo 144 da Constituição Federal, tem como atribuições a prevenção e repressão de infrações penais de competência da União, o combate ao tráfico ilícito de entorpecentes, contrabando e descaminho, além de atuar como polícia marítima, aeroportuária e de fronteiras. No âmbito da segurança portuária e aduaneira, a PF exerce papel central na investigação de crimes federais, na coordenação de ações de segurança em áreas portuárias, e na preservação da cadeia de custódia em ocorrências de ilícitos. Atua de forma integrada com a CONPORTOS/CESPORTOS, Receita Federal, Marinha do Brasil e ANTAQ, supervisionando a execução de planos de segurança, fiscalizando o cumprimento do ISPS Code, e coordenando operações especiais voltadas ao enfrentamento de ameaças como terrorismo, tráfico internacional, contrabando e cibercrimes, garantindo a legalidade e a proteção das infraestruturas críticas do sistema portuário nacional.

RECEITA FEDERAL DO BRASIL

A Receita Federal do Brasil (RFB), órgão de administração tributária e aduaneira vinculado ao Ministério da Fazenda, é responsável pelo controle aduaneiro de mercadorias, veículos e pessoas que ingressam ou saem do território nacional, assegurando o cumprimento da legislação fiscal e aduaneira, conforme o Decreto nº 6.759/2009 (Regulamento Aduaneiro). No contexto da segurança portuária e aduaneira, a RFB tem papel estratégico na prevenção e repressão de ilícitos como contrabando, descaminho, tráfico e fraude documental, além de garantir a integridade da cadeia logística internacional. É a autoridade competente para conceder o

Ato Declaratório Executivo (ADE) de Alfandegamento, que certifica o cumprimento dos requisitos de segurança exigidos pela Portaria RFB nº 143/2022 e pelas Portarias COANA nº 72, 75, 76 e 80/2022, relativas à infraestrutura, monitoramento e verificação remota de cargas. Atua também na implementação do Programa Operador Econômico Autorizado (OEA), reconhecendo intervenientes de baixo risco e fomentando o comércio seguro. Sua atuação é integrada com a Polícia Federal, ANTAQ, Marinha do Brasil, ANVISA e CONPORTOS/CESPORTOS, consolidando um sistema de fiscalização e segurança aduaneira voltado à proteção do Estado, à legalidade das operações e à credibilidade do comércio exterior brasileiro.

MARINHA DO BRASIL

A Marinha do Brasil, força integrante das Forças Armadas, subordinada ao Ministério da Defesa e regida pela Lei Complementar nº 97/1999, tem como uma de suas atribuições constitucionais a garantia da soberania nacional, da segurança da navegação e da defesa das águas jurisdicionais brasileiras. No contexto da segurança portuária e aduaneira, atua por meio das Capitanias dos Portos, Delegacias e Agências, responsáveis pela fiscalização do tráfego aquaviário, vistorias de embarcações, habilitação de tripulantes e prevenção da poluição hídrica por embarcações, conforme a Lei nº 9.537/1997 (Lei de Segurança do Tráfego Aquaviário – LESTA) e o Regulamento da LESTA (Decreto nº 2.596/1998). É também membro permanente da CONPORTOS/CESPORTOS, contribuindo tecnicamente para a avaliação de riscos e homologação dos Planos de Segurança Portuária (PSP), além de participar de inspeções conjuntas em instalações portuárias e terminais de uso privado. Sua atuação se dá de forma integrada com a Polícia Federal, Receita Federal, ANTAQ e ANVISA, garantindo o cumprimento das normas internacionais de segurança marítima, como o ISPS Code e a Convenção SOLAS, e fortalecendo a proteção das infraestruturas críticas e da navegação nos portos brasileiros.

MPOR

O Ministério de Portos e Aeroportos (MPOR), órgão da administração direta do Governo Federal, criado pela Lei nº 14.600/2023, é responsável pela formulação, coordenação e supervisão das políticas nacionais para o setor portuário e aeroportuário, atuando para promover a eficiência, segurança e competitividade da infraestrutura logística do país. No âmbito da segurança portuária e aduaneira, o MPOR exerce função estratégica de coordenação institucional, articulando-se com órgãos reguladores e fiscalizadores — como a ANTAQ, CONPORTOS, Receita Federal, Marinha do Brasil e Polícia Federal — para assegurar a conformidade das operações portuárias com os padrões de proteção e governança. Compete-lhe definir diretrizes de desenvolvimento e modernização dos portos, promover políticas de inovação, sustentabilidade e segurança operacional, além de supervisionar a administração portuária pública e a regulação dos terminais privados. O Ministério também apoia a implementação de programas voltados à digitalização de processos, resiliência cibernética e integração interagências, contribuindo para um sistema portuário nacional mais seguro, sustentável e competitivo.

CONPORTOS

A Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS), instituída pelo Decreto nº 9.861/2019, é um órgão colegiado, permanente e deliberativo, vinculado ao Ministério da Justiça e à Segurança Pública, com presidência exercida por um representante da Polícia Federal. Sua principal atribuição é estabelecer normas e diretrizes de segurança portuária, em conformidade com o Código Internacional para a Proteção de Navios e Instalações Portuárias (ISPS Code) e a Convenção SOLAS, garantindo a proteção de pessoas, cargas e instalações portuárias contra ameaças como terrorismo, sabotagem e tráfico ilícito. Compete à CONPORTOS homologar Estudos de Avaliação de Risco

(EAR) e Planos de Segurança Portuária (PSP), supervisionar auditorias, emitir Declarações de Cumprimento (DC) e coordenar a atuação das Comissões Estaduais de Segurança Pública nos Portos (CESPORTOS). Atua de forma integrada com a Polícia Federal, Marinha do Brasil, Receita Federal, ANTAQ e demais órgãos de segurança e fiscalização, promovendo a padronização dos procedimentos de proteção e o aperfeiçoamento contínuo da cultura de segurança nas instalações portuárias brasileiras.

CESPORTOS

A Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CESPORTOS) é o braço operacional da CONPORTOS nos estados, instituída pelo Decreto nº 9.861/2019, com a finalidade de implementar, fiscalizar e acompanhar as ações de segurança portuária em nível regional. Composta por representantes da Polícia Federal, Marinha do Brasil (Capitania dos Portos), Receita Federal, ANTAQ, Administrações Portuárias e Secretarias Estaduais de Segurança Pública, a CESPORTOS atua de forma colegiada na análise dos Estudos de Avaliação de Riscos (EAR) e dos Planos de Segurança Portuária (PSP), realizando inspeções e auditorias *in loco,* antes da homologação nacional pela CONPORTOS. É responsável por verificar a conformidade das instalações com o ISPS Code e as Resoluções da CONPORTOS, além de orientar os Supervisores de Segurança Portuária e coordenar ações integradas entre os órgãos de segurança pública. Sua atuação é essencial para a padronização das medidas de proteção, a prevenção de ilícitos e incidentes e para o fortalecimento da governança da segurança portuária nos portos e terminais brasileiros.

Compreendidos os principais atores que compõem o sistema de segurança portuária e aduaneira e suas respectivas formas de atuação, torna-se necessário analisar os riscos e vulnerabilidades que podem afetar o funcionamento seguro das instalações portuárias e das operações logísticas. Nesse sentido, o próximo capítulo

apresenta as principais ameaças associadas ao ambiente portuário, abordando diferentes tipos de ocorrências que podem comprometer a integridade das operações, das cargas, das infraestruturas e das pessoas envolvidas nas atividades portuárias e aduaneiras.

7- Ameaças e fraquezas na segurança

A segurança portuária e das áreas alfandegadas constitui um pilar essencial para a proteção do comércio internacional, da infraestrutura crítica e da integridade das cadeias logísticas globais. As instalações portuárias e alfandegadas, por sua natureza estratégica, estão expostas a uma ampla variedade de ameaças (de ordem externa), como terrorismo, furto, tráfico, contrabando e crimes cibernéticos, bem como a vulnerabilidades internas, decorrentes de fatores como falhas operacionais e treinamentos inadequados.

Este capítulo tem como objetivo apoiar gestores e responsáveis pela segurança na identificação clara e estruturada dessas ameaças e fraquezas. Diferentemente da etapa inicial do guia – voltada para a verificação do cumprimento da regulamentação vigente e da aderência às normas de segurança já estabelecidas – este momento do processo convida as instalações a olhar para dentro de suas operações, reconhecendo vulnerabilidades específicas do seu contexto físico, tecnológico e humano.

A partir dessa identificação, será possível compreender não apenas os riscos que comprometem a proteção do ambiente portuário e aduaneiro, mas também os pontos de fragilidade que podem ser explorados por agentes mal-intencionados. Tal diagnóstico é indispensável para orientar a aplicação das boas práticas que serão apresentadas no capítulo seguinte, assegurando que cada medida de mitigação seja direcionada às reais necessidades da instalação.
Assim, este capítulo representa a segunda etapa da metodologia proposta: um exercício crítico de autoconhecimento, no qual a análise das ameaças e fraquezas funcionará como base para o fortalecimento contínuo da segurança portuária e retroportuária.

São apresentadas as definições de cada ameaça/fraqueza, as formas e sinais para se reconhecer e casos práticos ocorridos em instalações portuárias, seja no Brasil, seja em outros países.

7.1 Terrorismo e Sabotagem

No Brasil, a definição de terrorismo encontra-se descrita na Lei nº13.260, de 16 de março de 2016, lei antiterrorismo:

> Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.
> § 1º São atos de terrorismo:
> I - Usar ou ameaçar, usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;
> II & III– (VETADOS);
> IV - sabotar o funcionamento ou apoderar-se, com violência, de grave ameaça à pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
> V - Atentar contra a vida ou a integridade física de pessoa.
> Pena - reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.
> § 2º O disposto neste artigo não se aplica à conduta individual ou coletiva de pessoas em manifestações políticas, movimentos sociais, sindicais, religiosos, de classe ou de categoria profissional, direcionados por propósitos sociais ou reivindicatórios, visando a contestar, criticar, protestar ou apoiar, com o objetivo de defender direitos, garantias e liberdades constitucionais, sem prejuízo da tipificação penal contida em lei (Brasil, 2016).

7.1.1 Casos de Terrorismo registrados no Brasil

Embora o Brasil não seja historicamente alvo de ataques terroristas, há registros de atos preparatórios e de promoção ao terrorismo. Em 2024, a Operação Mujahidin, conduzida pela Polícia Federal, investigou um indivíduo responsável por divulgar conteúdos de apologia ao terrorismo e incitação ao ódio religioso em redes sociais, com menções a grupos extremistas internacionais como Al-Qaeda e Estado Islâmico.[1]

1 A informação é constante de um compilado de casos divulgados pela Polícia Federal ao longo dos anos, a saber: Al-Qaeda (indícios apontados na Operação Mujahidin, em 2025 (Brasil, 2025), Hezbollah (indícios apontados na Operação Trapiche em 2023).

Outro caso emblemático foi a Operação Hashtag (2016), deflagrada às vésperas dos Jogos Olímpicos do Rio de Janeiro, com apoio do Federal Bureau of Investigation (FBI) dos Estados Unidos. A operação resultou na prisão de dez suspeitos de promover e incentivar ações vinculadas à organização extremista Estado Islâmico. As investigações apontaram que o grupo mantinha comunicação em redes sociais e aplicativos de mensagens, onde compartilhava conteúdos sobre táticas de ataque e incitava ações de "lobos solitários" contra atletas e delegações estrangeiras do Reino Unido, Estados Unidos e França (Brasil, 2018).

Os réus foram condenados por promover, entre março e julho de 2016, a organização terrorista Estado Islâmico do Iraque e do Levante (EILL) ou Estado Islâmico do Iraque e da Síria (EIIS) — também conhecida pelos acrônimos ISIS ou ISIL. Segundo decisão do TRF4, o grupo realizava publicações, trocas de materiais e diálogos em plataformas digitais, configurando crimes de promoção e associação à organização terrorista, conforme a Lei nº 13.260/2016.

A Operação Hashtag foi a primeira ação antiterrorismo conduzida com base nessa lei, marcando um avanço na política nacional de segurança e na cooperação internacional para o enfrentamento do extremismo violento.

7.1.2 Ameaças e riscos em infraestruturas críticas

Com a importância do Brasil no comércio internacional e as tensões políticas mundiais que podem afetar países aliados, o terrorismo é uma ameaça potencial, ainda que remota. Nesse contexto, os terminais portuários, por sua natureza estratégica, podem ser alvos de ataque, assim como navios de bandeiras internacionais durante sua atracação.

As possíveis ameaças terroristas em terminais podem incluir:

1. a introdução de materiais perigosos ou explosivos em contêineres de carga;
2. o ataque a instalações portuárias vitais;
3. ataques a navios atracados;
4. infiltração de terroristas disfarçados de funcionários ou visitantes;
5. ataques a subestações elétricas ou quaisquer outros tipos de ataques que possam causar vítimas ou inoperabilidade da instalação.

Um exemplo marcante ocorreu no Porto de Áden, no Iêmen. Enquanto o navio de guerra norte-americano USS Cole estava reabastecendo no porto, um pequeno barco carregado de explosivos, tripulado por dois membros da Al-Qaeda, aproximou-se do navio e detonou-se contra o casco (FBI, [2025?]).

7.1.3 Incidentes no Porto de Vila do Conde (Barcarena/PA)

Até o presente momento, não há registro documentado de atentados terroristas em portos brasileiros. No entanto, em junho de 2024, foi identificado um artefato explosivo a bordo de um navio atracado no Porto de Vila do Conde, em Barcarena (PA) (Esquadrão [...], 2024). O material, localizado dentro de uma mochila nas proximidades da embarcação, foi encontrado por tripulantes durante a operação de descarga de minérios.

A área foi isolada preventivamente, e o esquadrão antibombas da Polícia Militar do Pará, em conjunto com a Polícia Federal, atuou de forma imediata. Após a confirmação da presença de explosivos, o artefato foi detonado de maneira controlada, sem registro de feridos ou danos à infraestrutura portuária.

A pronta comunicação às autoridades competentes e a ausência

de intervenção de terceiros sobre o material foram fundamentais para evitar um incidente de maiores proporções. A Polícia Federal instaurou inquérito para investigar a origem e a autoria do artefato. Em síntese, a atuação correta, com o reporte imediato à Polícia Federal, sem qualquer intervenção de terceiros no material, evitou um incidente de maiores proporções.

7.1.4 Prevenção e resposta no setor portuário

A prevenção a atos terroristas nos portos exige a implementação de medidas de segurança rigorosas, em conformidade com o ISPS CODE.

Conforme já abordado, a certificação de uma instalação portuária pela CONPORTOS e os constantes treinamentos exigidos pela Resolução 53/2020 são os primeiros passos para um ambiente minimamente seguro.

Não basta, entretanto, que as medidas de segurança apontadas no Plano de Segurança Portuária (PSP) estejam em conformidade com o Estudo de Avaliação de Risco (EAR) e o ISPS CODE. É preciso que as medidas mitigadoras sejam eficientes e eficazes.

Para tanto, é necessário um treinamento constante, não só dos membros da área de segurança, mas também, de todos os colaboradores, objetivando que todos saibam os seus papéis e o que fazer nesses casos.

Segundo a ABIN (2020), entre os exemplos de indícios que, combinados, revelam sinais de possíveis planos terroristas em andamento, estão:

- Falsificação de documentos como passaporte, CPF, Carteira de Identidade, Carteira de habilitação, entre outros;
- Aquisição e manuseio de armas, munições, acessórios e equipamentos de uso restrito e sem a devida autorização;

↘Aquisição e manuseio não autorizados de produtos biológicos, químicos, nucleares, radiológicos de uso controlado;
↘Aquisição em larga escala de produtos de venda liberados, mas que podem ser utilizados para fabricação de explosivos, tais como acetona, água oxigenada, ácido sulfúrico, nitrato de amônia, entre outros;
↘Posse não autorizada de dados como imagens, vídeos, plantas, croquis, mapas, posicionamento de câmeras e vigilantes de alguma instalação pública ou privada de grande circulação;
↘Vínculo com organizações terroristas ou extremistas;
↘Envio de dinheiro a organizações terroristas ou extremistas;
↘Transferências de grandes somas de dinheiro para países onde há maior atuação de terroristas ou onde há zonas de conflito;
↘Tentativas de acesso não autorizado a áreas restritas de instalações públicas ou privadas de grande circulação;
↘Discursos extremados, inclusive em redes sociais, de ódio e incitação à violência;
↘Divulgação de ameaças, inclusive em redes sociais, de atentados terroristas.

Além da definição e normativas trazidas pelo ordenamento jurídico brasileiro em reação ao combate ao terrorismo, a Organização das Nações Unidas (ONU) também atua na sua prevenção, por meio da regulamentação de produtos que possam gerar Armas de Destruição em Massa (ADM), podendo ser nucleares, químicos, biológicos ou radiológicos. Tais conjuntos de itens são definidos como "bens sensíveis" e devem cumprir a Resolução da ONU 1.540, que foi adotada em 28 de abril de 2004 e é juridicamente vinculante para todos os Estados membros da ONU.

Após o atentado de 11 de setembro de 2001 às Torres Gêmeas, em Nova York, o governo e a Aduana dos EUA (*Customs and Border Protection*- CBP), temendo um novo incidente terrorista por meio de contaminação quando da importação de cargas ao adentrarem no território americano, em 2002, implementaram o Programa de Segurança *Customs-Trade Partnership Against Terrorism* - C-TPAT, que consiste na inspeção, por parte da fiscalização aduaneira da CBP, de toda a cadeia logística desde o país de origem até a chegada e desembaraço aduaneiro nos Estados Unidos.

Para que pudesse obter dados, informações e acesso a procedimentos de outras Aduanas globalmente para alcance deste mapeamento, a CBP instituiu o Programa de Acordos Internacionais denominado *Container Security Iniciative* (CSI), em que os países exportadores permitem a instalação permanente de unidades da CBP junto às Alfândegas desses países, em ação compartilhada com a Aduana americana, que permite a inspeção conjunta de contêineres ainda no local do embarque, com a utilização de equipamentos na modalidade não invasiva (escâner de contêiner e detector de radiação), selecionados com base em análise dos documentos de transporte e informações lançadas nos sistemas de controle e Despachos Aduaneiros da CBP, fornecidas antecipadamente pelos agentes marítimos, exportadores estrangeiros, bem como pelos importadores norte-americanos.

Esses são exemplos de regramentos a serem cumpridos por meio dos controles, quando há a confirmação do atendimento das etapas da cadeia logística no Comércio Internacional, no que dizem respeito ao manuseio das cargas; à análise documental e, principalmente, ao controle, tratamento e comunicação das informações, com a maior antecedência possível, permitindo o estabelecimento de gerenciamento de risco sobre cada operação de compra e venda/ transferências de cargas entre os países.

Com isso, as empresas e os órgãos intervenientes adotam essas ações preventivas as quais permitem maior precisão na análise de risco e gestão aduaneira pelas Aduanas, contra o Comércio Internacional de ADM e Bens Sensíveis que possam viabilizar e subsidiar qualquer atividade terrorista.

7.1.5 Sabotagem e riscos internos

A sabotagem consiste em danificar, destruir ou obstruir deliberadamente sistemas, equipamentos ou processos, com o

objetivo de interromper ou prejudicar operações. Pode ter motivação política, econômica, ideológica ou pessoal, e ocorrer de forma física, cibernética ou organizacional.

Um funcionário insatisfeito pode representar risco de sabotagem por fatores como falta de reconhecimento, remuneração inadequada ou conflitos interpessoais. Além disso, o conhecimento interno sobre processos e vulnerabilidades torna esse tipo de ameaça especialmente perigoso.

A insatisfação pode surgir de questões como falta de reconhecimento, remuneração inadequada, sobrecarga de trabalho, falta de oportunidades de crescimento, conflitos interpessoais, entre outros fatores.

Essa insatisfação pode levar o funcionário a se sentir desmotivado, desvalorizado e até mesmo ressentido em relação à empresa. Como resultado, ele pode agir de maneira sabotadora, como uma forma de expressar sua frustração, buscar vingança ou tentar chamar a atenção para suas demandas não atendidas. Além disso, o conhecimento dos processos internos e vulnerabilidades da empresa pelo colaborador ou por um terceirizado pode fragilizar sobremaneira a instalação.

Essa ameaça está associada ao risco de que esses profissionais realizem ou contribuam para incidentes de segurança, aproveitando-se do acesso autorizado que possuem, o que lhes confere uma vantagem estratégica.

Esses incidentes podem ocorrer por desconhecimento, negligência ou má-fé. A falta de informação sobre normas de segurança ou a postura negligente em relação às diretrizes pode levar à facilitação involuntária de ações ilícitas. Já os colaboradores mal-intencionados,

que atuam de forma deliberada, podem ser motivados por fatores diversos, como ganhos financeiros, ideologia, vingança, coerção ou desejo de reconhecimento.

Um colaborador pode ser recrutado com a intenção de causar danos, ou pode ser influenciado ao longo do tempo para agir contra a organização, sendo cooptado por terceiros.

Esses colaboradores podem praticar ou facilitar diversos tipos de incidentes: desde a destruição de embarcações, introdução de armas ou dispositivos perigosos, vazamento de informações confidenciais, até o auxílio no acesso indevido a áreas restritas ou sistemas tecnológicos.

Para mitigar esses riscos, é essencial que as organizações adotem políticas robustas de segurança de pessoal, com medidas que visem a prevenir o recrutamento de indivíduos com histórico de risco; reduzir a possibilidade de que colaboradores se tornem ameaças; dificultar a ocorrência de atividades internas maliciosas e proteger os ativos organizacionais de forma sistêmica e contínua (IMO, 2024).

Essas ações de sabotagem podem incluir desde a propagação de boatos, atrasos deliberados em projetos, descumprimento de prazos, danos físicos ou virtuais à empresa e a pessoas. Justamente por essas razões, as áreas mais sensíveis de uma IP são classificadas, dependendo do seu grau de importância, como restritas ou controladas.

As áreas mais sensíveis (restritas) devem possuir controle de acesso com dupla camada de segurança, a fim de restringir ao máximo o acesso de pessoas não autorizadas ou controlar quem as utiliza.

Portanto, é importante que as organizações estejam atentas aos sinais de insatisfação dos funcionários e busquem abordar as causas

subjacentes para evitar possíveis atos de sabotagem e manter um ambiente de trabalho saudável e produtivo.

7.2 Passageiros clandestinos

A Convenção para a Facilitação do Tráfego Marítimo Internacional de 1965, promulgada pelo Decreto 80.672/1977, traz em suas emendas a definição de passageiro clandestino:

> Uma pessoa que esteja escondida num navio, ou numa carga que seja posteriormente embarcada num navio, sem o consentimento do armador, do comandante ou de qualquer outra pessoa responsável, e que seja descoberta a bordo do navio depois que ele tenha saído do porto, ou na carga enquanto ela estiver sendo descarregada no porto de chegada, e que seja informada pelo comandante ou pelas autoridades competentes como sendo um clandestino (Brasil, 2021).

Em 2019, a IMO publicou a FAL 43/13, trazendo uma análise dos riscos e custos relacionados aos casos de passageiros clandestinos no mundo (IMO, 2019). Para se ter uma ideia, em 2017, o número de passageiros clandestinos contabilizados foi de 1.420, um crescimento de 11,4%, quando comparado com 2014. Os dados também demonstram que a maioria desses passageiros tinham como país de origem a Nigéria e Tanzânia.

No Brasil, igualmente, têm sido registradas ocorrências envolvendo passageiros clandestinos. A título ilustrativo, em 2021, no Porto de Paranaguá, foi identificado um estrangeiro que buscava ingressar de maneira irregular no território nacional, ocultando-se a bordo de um navio cargueiro. O indivíduo, que declarou ser natural da Guiné, teria embarcado sem a devida autorização em embarcação que realizara escala no Porto de Dakar, Senegal (Brasil, 2021).

A presença de passageiros clandestinos a bordo das embarcações representa uma ameaça significativa, não apenas para a segurança da tripulação e das operações portuárias, mas também para a estabilidade comercial dos armadores e operadores. Esses casos

costumam ser demorados e complexos, envolvendo múltiplas partes interessadas e podendo acarretar implicações jurídicas, financeiras e diplomáticas. Além disso, o comportamento de clandestinos pode se tornar hostil em relação à tripulação do navio e aos terminais nos quais a embarcação se encontra atracada, aumentando os riscos para todos os envolvidos.

As ações de prevenção contra passageiros clandestinos estão mais diretamente relacionadas às práticas adotadas pelas embarcações do que pelos terminais portuários em si. Nesse sentido, é fundamental que os navios realizem avaliações de vulnerabilidade e risco, assegurando que o plano de segurança do navio contemple medidas específicas para impedir o acesso de potenciais clandestinos.

No entanto, algumas boas práticas também podem ser realizadas pelos terminais, a fim de garantir a maior segurança no desembarque (ou não) desses passageiros. Tais boas práticas são identificadas no capítulo 8 deste guia.

Faz-se imperioso suscitar que a "tentativa de imigração não autorizada" , a princípio, não configura prática de crime, exceto para quem a promove com o intuito de lucro[2].

Trata-se de uma pessoa que não deveria estar no local ou no navio, e que poderia ter relação com algum dos crimes relatados neste capítulo, apenas se esse indivíduo for o autor partícipe dessas

2 Código Penal - **Promoção de migração ilegal.** "Art. 232-A. Promover, por qualquer meio, com o fim de obter vantagem econômica, a entrada ilegal de estrangeiro em território nacional ou de brasileiro em país estrangeiro:
Pena - reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
§ 1º Na mesma pena incorre quem promover, por qualquer meio, com o fim de obter vantagem econômica, a saída de estrangeiro do território nacional para ingressar ilegalmente em país estrangeiro.
§ 2º A pena é aumentada de 1/6 (um sexto) a 1/3 (um terço) se:
I - o crime é cometido com violência; ou
II - a vítima é submetida a condição desumana ou degradante.
§ 3º A pena prevista para o crime será aplicada sem prejuízo das correspondentes às infrações conexas." (Brasil, 1940).

ilegalidades.

Assim, para fins da Segurança Portuária e Aduaneira, seria "*uma pessoa não autorizada dentro de um veículo ou desembarcado em um terminal portuário*", isto é, não é um passageiro regular, tampouco um tripulante identificado na relação do navio apresentada antecipadamente junto às autoridades. Nessa condição, a agência marítima e o Terminal são obrigados a proceder com a comunicação desse fato para Polícia Federal, responsável pelo controle de imigração, para a autoridade aduaneira, e para demais autoridades. A não observância configura infração aos controles aduaneiros e migratórios, estabelecidos pelas normas brasileiras.

7.3 Roubo, Furto de Carga e Extorsão

Tipicamente, o roubo exige o emprego de ameaça e violência, por exemplo, com uso de arma no sentido amplo, em contraposição, o crime de furto é descrito como subtração de bens sem o emprego de violência, conforme pode ser observado pela definição do Código Penal Brasileiro:

> **Furto**
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> **Roubo**
> Art. 157 - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência:
> Pena - reclusão, de quatro a dez anos, e multa (Brasil, 1940).

Nos terminais portuários e recintos aduaneiros, onde existem intensos fluxos de usuários, colaboradores e terceiros intervenientes, tais crimes podem ser praticados por quaisquer dessas pessoas, mas para o proprietário da carga, a consequência é verificada com o dever de reparar o dano sofrido, sendo a Responsabilidade Civil atribuída ao terminal depositário e/ou operador das cargas, tanto em relação ao proprietário das cargas como perante as Autoridades

Intervenientes, independente da tipificação da prática criminal e da autoria do crime ter sido praticada por colaborador do terminal ou não.

Daí decorre a necessidade de implantação, por parte das Administradoras dos terminais portuários, de várias medidas preventivas e mitigatórias quanto à prática do crime de roubo ou furto de cargas dentro de suas instalações, onde ele é o "fiel depositário", segundo a legislação brasileira.

É importante ressaltar que roubos e furtos de cargas podem se dar em diversos momentos da cadeia logística. Algumas das principais modalidades de roubo/furto de cargas são:

I - Roubo Durante o Transporte	Ocorre quando os criminosos atacam os caminhões ou contêineres durante o transporte da carga para o terminal ou instalação alfandegada.
Exemplo: Sequestro de veículos de transporte.	
II - Roubo ou furto no interior da Instalação Portuária e Alfandegada	Envolve a abertura não autorizada de contêineres e o saque das mercadorias.
Exemplo: Uso de ferramentas para abrir contêineres ou adulteração de lacres.	
III - Envolvimento com Funcionários Internos	**Método 1:** Envolvimento de colaboradores que facilitam a subtração por meio de ações internas.
Exemplo: Alteração de documentos para desviar mercadorias ou facilitação de acesso não autorizado.	
	Método 2: Roubo de cargas/mercadorias em trânsito entre o navio e o local de armazenamento.
Exemplo: Ataques a embarcações em hidrovias.	
IV - Fraude e Manipulação de Documentos	Método: Manipulação de documentos para desvios de carga.

Um dos roubos mais famosos ocorreu no Porto de San Antônio, no Chile, em 2023. Um grupo armado levou 13 contêineres cheios

de cobre, que juntos somavam mais de 4 milhões de dólares. Os assaltantes desligaram as câmeras e intimidaram os guardas e os trabalhadores de dentro do terminal.

No Comércio Internacional realizado pelos Terminais Portuários brasileiros, o roubo de carga depositada ou em Trânsito Aduaneiro pode se dar com:

- mercadoria estrangeira em importação;
- mercadoria estrangeira em Trânsito Aduaneiro;
- mercadoria nacional/estrangeira em exportação;
- mercadoria nacional em Trânsito Aduaneiro.

Os desdobramentos traçados são determinantes para delimitação das responsabilidades tributárias e de controle aduaneiro.
No regramento nacional, os tributos são devidos pela mercadoria registrada perante o Siscomex, mesmo que eventualmente não sejam localizadas, isto é, quando ocorre o roubo os tributos são devidos de qualquer modo.

Questiona-se o porquê da tributação quando da prática do roubo de carga. A legislação aduaneira/tributária vigente define procedimentos de atuação da fiscalização, quando da verificação da falta de mercadoria registrada, mesmo com a suspeita ou alegação de roubo, em que presumidamente o produto que adentrou ao território brasileiro poderia ser comercializado no mercado interno sem o recolhimento dos tributos incidentes na importação/exportação e os demais tributos internos. A exceção é a comprovação de "erro de declaração", também considerado como "vício de origem", mesmo assim, existe a aplicação de multa decorrente da ausência ou erro de prestação de informações elementares, que prejudicam o controle aduaneiro.

Faz-se válido considerar que o controle aduaneiro verifica

diariamente importadores/exportadores os quais imputam de má-fé informações junto ao Siscomex quanto à carga, como erro na classificação fiscal pelos código descritos pela NESH/NCM e/ou, em quantidades maior ou menor de mercadorias para afastar o recolhimento dos tributos proporcionais a esses, e, até mesmo, para reclamarem indenizações indevidas. Diante disso, ao tratar do tema do "roubo de carga" dentro do contexto da Segurança Aduaneira, é imperiosa a constatação, por meio de provas contundentes, da prática do referido crime.

Outra vulnerabilidade em segurança é a possibilidade de colaboradores ou terceirizados que atuem em determinada instalação sofrerem extorsão. Em tese, quaisquer pessoas com acesso a informações sensíveis ou úteis para organizações criminosas podem ser vítimas de tal crime, que pode se dar por um ato de violência, grave ameaça ou até mesmo chantagem. Por isso, uma das grandes vulnerabilidades é o funcionário insatisfeito.

O crime de extorsão está previsto no código Penal em seu artigo 158:

> **Art. 158** - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: Pena - reclusão, de quatro a dez anos, e multa (Brasil, 1940).

No contexto deste trabalho, o referido crime é considerado um intermediário/meio para a prática dos demais crimes tratados neste capítulo, que podem ocorrer nos Terminais Portuários e instalações alfandegadas, comprometendo a Segurança do Porto ou da carga. A adoção das boas práticas, no aspecto da Segurança Portuária e Aduaneira, diz respeito a medidas preventivas relacionadas aos recursos humanos quando da contratação, treinamento e designação dos ocupantes de determinados cargos, identificados como sensíveis e estratégicos à atuação criminosa. Essas boas práticas são melhores descritas no capítulo seguinte.

7.4 Tráfico, Descaminho e Contrabando

Inicialmente, faz-se fundamental trazer o conceito de três figuras distintas, que apresentam enquadramento penal próprio, mas que são frequentemente confundidas entre si: o tráfico, o descaminho e o contrabando.

Tem-se como tráfico em sentido amplo a circulação ilícita de mercadorias, enquanto no sentido estrito é a comercialização, transporte, importação ou exportação de bens, pessoas ou substâncias cuja circulação é proibida ou restrita por lei. Assim, a lei realiza tipificação da conduta de acordo com o objeto do tráfico (ex.: tráfico de drogas, tráfico de pessoas, tráfico de armas etc.).

O tráfico de drogas, por exemplo, é tipificado na Lei 11.343/2006, já o tráfico de pessoas, no Código Penal, e o tráfico de armas, pelo estatuto do desarmamento (Lei 10.826/2003).

Um dos incidentes de proteção mais presentes no dia a dia das instalações portuárias é o tráfico de entorpecentes.

Os métodos mais utilizados pelos traficantes são:

Rip on- Rip off loading:	A carga lícita de empresa idônea é contaminada com cocaína por meio do desvio na rota do contêiner, durante a estufagem ou mesmo dentro dos terminais enquanto aguarda embarque.
Carga montada:	Utiliza-se de empresa exportadora e importadora "laranja". É montada uma exportação somente para envio da droga. É feito por meio do uso de cargas mais elaboradas, com certo grau de sofisticação na ocultação da droga.

Içamento:	São utilizados barcos para levar a carga de entorpecentes até o navio, onde trabalhadores portuários ou mesmo membros da tripulação realizam o içamento, puxando as drogas para o navio e escondendo-as em cargas ou compartimentos da embarcação, para retirada no porto de destino. Pode ser realizado com o navio atracado ou na área de fundeio.
Barrigada:	Trabalhadores portuários adentram ao Terminal em seus turnos de trabalho, trazendo consigo, presos ao corpo por uma cinta elástica, tabletes de cocaína que serão introduzidos em contêiner ou outro local, a bordo do navio.
Mergulhadores:	Mergulhadores anexam bolsas com drogas junto ao casco do navio (seachest), as quais ficam submersas até a retirada pela Organização Criminosa no porto de destino.

Portanto, no presente contexto, o crime de tráfico é em relação ao comércio ilícito, mais especificamente, de mercadoria ilícita, decorrente de previsão pela legislação brasileira.

Já o crime de Descaminho é o comércio de bens lícitos, mas de forma não regularmente apresentada para desembaraço aduaneiro. É prática contra a ordem tributária[3], por meio de introdução no território nacional de mercadoria estrangeira lícita ou a saída de mercadoria brasileira lícita, sem adoção do regular procedimento de importação ou de exportação, o que impede o lançamento do

3 Descaminho. "Art. 334. Iludir, no todo ou em parte, o pagamento de direito ou imposto devido pela entrada, pela saída ou pelo consumo de mercadoria (Redação dada pela Lei nº 13.008, de 26.6.2014)
Pena - reclusão, de 1 (um) a 4 (quatro) anos. (Redação dada pela Lei nº 13.008, de 26.6.2014)
§ 1o Incorre na mesma pena quem: (Redação dada pela Lei nº 13.008, de 26.6.2014)
I - pratica navegação de cabotagem, fora dos casos permitidos em lei; (Redação dada pela Lei nº 13.008, de 26.6.2014)
II - pratica fato assimilado, em lei especial, a descaminho; (Redação dada pela Lei nº 13.008, de 26.6.2014)
III - vende, expõe à venda, mantém em depósito ou, de qualquer forma, utiliza em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria de procedência estrangeira que introduziu clandestinamente no País ou importou fraudulentamente ou que sabe ser produto de introdução clandestina no território nacional ou de importação fraudulenta por parte de outrem; (Redação dada pela Lei nº 13.008, de 26.6.2014)
IV - adquire, recebe ou oculta, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria de procedência estrangeira, desacompanhada de documentação legal ou acompanhada de documentos que sabe serem falsos. (Redação dada pela Lei nº 13.008, de 26.6.2014)
§ 2o Equipara-se às atividades comerciais, para os efeitos deste artigo, qualquer forma de comércio irregular ou clandestino de mercadorias estrangeiras, inclusive o exercido em residências. (Redação dada pela Lei nº 13.008, de 26.6.2014)
§ 3o A pena aplica-se em dobro se o crime de descaminho é praticado em transporte aéreo, marítimo ou fluvial. (Redação dada pela Lei nº 13.008, de 26.6.2014"

crédito tributário, uma vez que a RFB não teve acesso à existência/ocorrência do fato gerador do tributo.

É ampla a gama de casos de drogas apreendidas em terminais portuários e recintos alfandegados. Segundo o relatório publicado pela Escritório das Nações Unidas sobre Drogas e Crime (UNODC), em 2025, os traficantes dependem das rotas marítimas para mais de 90% das remessas (UNODC, 2025). Já o descaminho e o contrabando são tipificados nos Artigos 334 e 334-A do Código Penal Brasileiro:

> **Descaminho**
> Art. 334. Iludir, no todo ou em parte, o pagamento de direito ou imposto devido pela entrada, pela saída ou pelo consumo de mercadoria.
> **Contrabando**
> Art. 334-A. Importar ou exportar mercadoria proibida (Brasil, 1940).

Assim é afastado o recolhimento dos tributos envolvidos na operação ou o cumprimento de controles administrativos, mediante subterfúgio de não apresentação para o Despacho Aduaneiro.

Por outro lado, o crime de Contrabando é a importação ou exportação de mercadoria proibida pela legislação aduaneira[4], nem sempre ilícita, como por exemplo, bens usados, armas e explosivos (dependem de autorização prévia), cigarros e remédios (dependem de controle sanitário), entre outros produtos controlados. Não ocorre a apresentação da mercadoria para o regular Despacho Aduaneiro

4 "Contrabando. Art. 334-A. Importar ou exportar mercadoria proibida: (Incluído pela Lei nº 13.008, de 26.6.2014)
Pena - reclusão, de 2 (dois) a 5 (cinco) anos. (Incluído pela Lei nº 13.008, de 26.6.2014)
§ 1o Incorre na mesma pena quem: (Incluído pela Lei nº 13.008, de 26.6.2014)
I - pratica fato assimilado, em lei especial, a contrabando; (Incluído pela Lei nº 13.008, de 26.6.2014)
II - importa ou exporta clandestinamente mercadoria que dependa de registro, análise ou autorização de órgão público competente; (Incluído pela Lei nº 13.008, de 26.6.2014)
III - reinsere no território nacional mercadoria brasileira destinada à exportação; (Incluído pela Lei nº 13.008, de 26.6.2014)
IV - vende, expõe à venda, mantém em depósito ou, de qualquer forma, utiliza em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria proibida pela lei brasileira; (Incluído pela Lei nº 13.008, de 26.6.2014)
V - adquire, recebe ou oculta, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, mercadoria proibida pela lei brasileira. (Incluído pela Lei nº 13.008, de 26.6.2014)
§ 2º - Equipara-se às atividades comerciais, para os efeitos deste artigo, qualquer forma de comércio irregular ou clandestino de mercadorias estrangeiras, inclusive o exercido em residências. (Incluído pela Lei nº 4.729, de 14.7.1965)
§ 3o A pena aplica-se em dobro se o crime de contrabando é praticado em transporte aéreo, marítimo ou fluvial. (Incluído pela Lei nº 13.008, de 26.6.2014)".

nos locais autorizados de carregamento ou descarregamento em veículo procedente do exterior ou a ele destinado.

Os crimes de descaminho e de contrabando são puníveis na esfera civil/aduaneira com a perda da mercadoria, que poderá ser destinada, a depender do tipo, para leilão, doação, incorporação ou destruição pela Receita Federal do Brasil. Na esfera penal, o autor responderá aos crimes em processo criminal, o qual poderá resultar na perda da liberdade.

7.5 Espionagem Industrial

Para minimizar os riscos de espionagem econômica em ambientes portuários, é fundamental adotar medidas de segurança proativas e estratégias de proteção da informação.

Importante destacar que com um mundo cada vez mais digital, os riscos de espionagem neste ambiente passam a ser mais cibernéticos do que propriamente realizados por pessoas no ambiente físico. Esses riscos serão abordados no item sobre cibersegurança.

No Brasil, não existe um tipo penal específico chamado "espionagem industrial", no entanto, existem condutas específicas ligadas a esse conceito e que são tipificadas, a exemplo da violação de segredo industrial (Lei 9.279/1996), da concorrência desleal (com uso indevido de informações sigilosas), e da violação de segredo profissional (Art.154, do Código Penal).

Em nível internacional também é interessante trazer o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (Acordo TRIPS). O acordo estabelecido entre membros da OMC estabelece padrões mínimos para a proteção e aplicação de direitos de propriedade intelectual, como patentes, marcas, direitos autorais e segredos comerciais.

No ambiente portuário e aduaneiro, a espionagem industrial pode ocorrer como: obtenção ilícita de planos logísticos de empresas concorrentes, acesso indevido a informações de importações e exportações, acesso a imagens de câmeras dos terminais de forma a obter segredos quanto à operação, entre outros.

Para se ter uma ideia do avanço das tecnologias ligadas à espionagem industrial, o Comitê de Segurança Interna da Câmara dos Representantes dos EUA divulgou, em setembro de 2024, um relatório investigativo que mostrava como os guindastes, produzidos no exterior, e utilizados em terminais portuários, podem incorporar tecnologias que permitem o acesso secreto às máquinas portuárias, tornando-as vulneráveis à espionagem e à interrupção de operações (Green; Moolenaar; Gimenez, 2024).

A investigação revelou casos reais em que os guindastes vieram com modems de celulares instalados sem o conhecimento das autoridades portuárias e fora do escopo dos contratos.

O objetivo da espionagem industrial é obter uma vantagem competitiva, prejudicar o comércio ou interromper as cadeias de suprimentos, impactando as economias nacionais.

Ao promover uma cultura organizacional voltada para a proteção dos ativos e informações da empresa, é possível reduzir significativamente os riscos associados à espionagem econômica nas instalações portuárias.

Quando se trata do risco de espionagem feita por funcionários insatisfeitos, a situação se torna ainda mais delicada. É importante abordar essa questão com sensibilidade e estratégias específicas para lidar com esse tipo de ameaça interna.

7.6 Treinamento inadequado

O treinamento inadequado na área de segurança de uma instalação portuária é uma fraqueza que pode acarretar uma série de vulnerabilidades, as quais serão destacadas na sequência.

- **Falhas na identificação de ameaças:** Funcionários mal-treinados podem não ser capazes de identificar corretamente possíveis ameaças à segurança da instalação portuária, o que pode resultar em brechas de segurança não detectadas.
- **Utilização inadequada de equipamentos e tecnologias:** A falta de treinamento adequado pode levar a erros na utilização de equipamentos de segurança e tecnologias específicas da instalação portuária, comprometendo a eficácia dessas ferramentas. Nesse contexto, podemos citar, a título exemplificativo, a falta de treinamento em operadores de monitoramento de câmeras. Isso pode ocasionar a falta de identificação de criminosos no ambiente ou ainda a inabilidade no acompanhamento do intruso pelas câmeras.
- **Procedimentos inadequados em emergências:** Em casos de emergência, como incêndios, vazamentos ou invasões, funcionários sem treinamento adequado podem não saber como agir corretamente, colocando em risco a segurança de todos na instalação.
- **Vulnerabilidades na proteção de dados sensíveis:** Um treinamento deficiente em segurança da informação pode resultar em falhas na proteção de dados sensíveis da instalação portuária, tornando as informações vulneráveis a acessos não autorizados. Exemplo: Acessar um *link* malicioso encaminhado por *e-mail*.
- **Desconhecimento das políticas e procedimentos de segurança:** Funcionários que não recebem um treinamento claro sobre as políticas e procedimentos de segurança da instalação podem, inadvertidamente, violar regras importantes, comprometendo a integridade do ambiente. Sublinhe-se que o treinamento em ISPS CODE deve ser realizado não só pela equipe patrimonial, mas por todos os colaboradores, incluindo a gerência e diretoria da IP.
- **Aumento do Risco de Acidentes e Incidentes**: A falta de capacitação adequada em questões de segurança pode resultar em um aumento do número de acidentes e incidentes na instalação portuária, colocando em perigo a vida dos funcionários e o bom funcionamento das operações.

7.7 Ciberataque

O setor portuário enfrenta ameaças cibernéticas crescentes que são abordadas por duas perspectivas regulatórias complementares, cada uma com foco e metodologias específicas. A Organização Marítima Internacional (IMO) concentra-se na segurança marítima global por meio de *frameworks* normativos e diretrizes de gestão de riscos cibernéticos aplicáveis ao transporte marítimo e operações portuárias. Paralelamente, as autoridades aduaneiras focam na

proteção dos sistemas de controle do comércio exterior, enfatizando a prevenção de crimes que exploram vulnerabilidades cibernéticas para facilitar atividades ilícitas como tráfico de drogas, contrabando e evasão fiscal.

Ataques Cibernéticos são tentativas maliciosas e deliberadas para violar sistemas de informação com objetivo de danificar, roubar ou fazer uso não autorizado de ativos digitais.

> Ataque Cibernético é um evento lançado contra um alvo com a intenção de bloquear, interromper, destruir ou explorar um ambiente operacional de computador. Muitos ataques cibernéticos visam comprometer, explorar ou destruir a integridade dos dados alvo, roubar dados ou manipulá-los para fins maliciosos (IAPH, 2021, p.75, tradução nossa).

Os ataques cibernéticos no setor portuário podem ter impactos operacionais (paralisação da operação, alteração nos agendamentos), financeiros (perda de faturamento, custos com resgates), reputacionais (perda de confiança por parte dos clientes) e até mesmo de segurança nacional (riscos para a cadeia de suprimentos, exposição das fronteiras).

A Agência da União Europeia para Cibersegurança (ENISA, 2023) divide as ameaças cibernéticas nas seguintes categorias:

1. **Engenharia Social** – Exploram pessoas. Os ataques se aproveitam da fraqueza humana, manipulando usuários a cometerem erros ou revelarem informações sensíveis.

2. **Malware** - Programas desenvolvidos para infectar, danificar ou controlar sistemas.
3. **Negação de Serviço** - Visa a sobrecarregar os servidores de um terminal para tornar seus sistemas inoperantes, causando danos financeiros e de reputação.
4. **Ataques a Credenciais** - Tentativas de roubar ou adivinhar senhas e acessos.
5. **Falhas de Aplicações/Redes** - Exploram vulnerabilidades técnicas em *softwares*, protocolos ou configurações.

6. **Roubo e Espionagem** - Envolvem exfiltração e exploração de dados sensíveis para fins financeiros, políticos ou estratégicos.

O quadro a seguir apresenta os principais tipos de ataques, de acordo com as categorias exploradas acima:

Quadro 1 - Tipos de ataque

Engenharia Social

Phishing	Envolve o envio de e-mails fraudulentos para enganar funcionários e obter acesso a sistemas críticos. O usuário é induzido a clicar em links, abrir anexos ou fornecer dados pessoais. O phishing é um dos ataques mais comuns e perigosos, porque explora o fator humano. Mesmo a melhor infraestrutura de segurança pode ser comprometida se um funcionário for enganado.
Spear Phishing	Phishing direcionado a uma vítima ou organização específica.
Social Engineering	Manipulação psicológica das pessoas para burlar controles de segurança.
Spam	Envio em massa de mensagens não solicitadas para enganar ou induzir cliques.
Insider Threat	Funcionários/terceiros maliciosos ou descuidados explorando acesso legítimo.

Malware

Malware (genérico)	Termo guarda-chuva para *softwares* maliciosos, isto é, programas ou códigos que realizam operações não autorizadas com impacto negativo na confidencialidade, integridade ou disponibilidade de sistemas.
Ransomware	Tipo de *malware* que bloqueia ou criptografa arquivos ou sistemas, exigindo um resgate para restaurar o acesso ou evitar exposição dos dados. Continua sendo uma das ameaças mais impactantes. Segundo a ENISA (2025), 68% das intrusões resultam em implantação de *malware*, e a combinação de *ransomware*, trojans bancários e *infostealers* corresponde a 87,3**%** dos códigos maliciosos implantados após invasões.
Trojan Horse	Programa malicioso que se disfarça como *software* legítimo para induzir o usuário a executá-lo. Pode abrir *backdoors*, instalar outros *malwares* ou exfiltrar dados.

Vírus	Tipo de *malware* que se insere em outro programa, reproduz a si mesmo e infeta outros programas. Precisa da execução de um programa hospedeiro para se ativar.
Worm	Autorreplicante, espalha-se sozinho em redes, sem necessidade de intervenção humana. *Phishing* é vetor em cerca de 60% dos casos de infecção, e a exploração de vulnerabilidades representa 21,3% (ENISA, 2025).
Spyware	Programa oculto que monitora e coleta dados do usuário, como senhas, histórico, teclas digitadas e informações sensíveis, sem o seu conhecimento.
Droppers	Programa leve cujo objetivo é instalar ou "carregar" outros *malwares* no sistema, agindo como vetor inicial para ataques mais complexos.
Bot	Dispositivo infectado que recebe comandos remotos de um atacante (controlador), podendo executar atividades coordenadas, como ataques DDoS, mineração e spam. Botnets foram responsáveis por 9,9% dos vetores de intrusão observados (ENISA, 2025).

Negação de Serviço

Denial of Service (DoS)	Sobrecarga de um sistema a partir de uma única origem.
Distributed Denial of Service (DDoS)	Ataque semelhante ao DoS, porém, realizado simultaneamente por milhares de endereços IP únicos.

Ataques a credenciais

Brute Force Attack	O atacante realiza repetidas tentativas de senhas até acertar.

Ataques a aplicações e redes

Cross-Site Scripting (XSS)	Injeção de *scripts* em páginas web. O invasor injeta *scripts* maliciosos em páginas vistas por outros usuários, permitindo o roubo de informações.
Cross-Site Request Forgery (CSRF)	Engana usuários autenticados a executar ações indesejadas.
SQL Injection	Inserção de comandos SQL maliciosos em entradas de dados.
Man-in-the-Middle (MitM)	Intercepta comunicações entre vítima e servidor.
Domain Hijacking	Sequestro de domínio para assumir controle.

Spoofing (genérico)	Falsificação de identidade (IP, *e-mail* etc.). O invasor tenta se passar por uma entidade confiável para ocultar sua verdadeira identidade.
DNS Spoofing	Manipulação de DNS para redirecionar usuários para sites falsos, interceptar comunicações ou realizar ataques de intermediário.

Roubo e Espionagem

Advanced Persistent Threat (APT)	Ataques sofisticados e persistentes, ligados à espionagem.
Data Breach	Vazamento de dados sensíveis.
Exfiltration	Extração não autorizada de informações de um sistema.

Os ataques cibernéticos a terminais portuários e infraestruturas críticas têm se tornado mais frequentes em todo o mundo.

Em novembro de 2023, um incidente na DP World Austrália paralisou as operações em quatro grandes portos – Sydney, Melbourne, Brisbane e Fremantle –, afetando cerca de 40 % do fluxo de mercadorias do país (DP world [...], 2023). No mesmo ano, o Porto de Nagoya (Japão) foi alvo de um ataque de *ransomware* que suspendeu a movimentação de contêineres e a exportação de veículos, impactando especialmente a Toyota Motor Corporation (Lyngaas, 2023). Esses episódios evidenciam a vulnerabilidade das cadeias logísticas globais e a necessidade de estruturas robustas de cibersegurança no setor portuário.

Segundo o Relatório de Ameaças Cibernéticas da Fortinet (2024), o Brasil foi o país mais atacado da América Latina, concentrando 36% de todos os incidentes registrados na região, o que corresponde a mais de 23 bilhões de tentativas de ataque. Dados da Check Point (2025) confirmam que o Brasil continua entre os 10 países mais visados globalmente, com uma média de 1.158 ataques por semana por organização. A ENISA (2025) também destaca que o setor de transporte e logística está entre os cinco mais afetados globalmente,

com *ransomware* e *infostealers* entre as principais ameaças.

Embora os incidentes específicos em terminais portuários sejam menos divulgados, a crescente digitalização e a automação das operações tornam os portos brasileiros alvos estratégicos para cibercriminosos.

Em 2019, o Porto de Mucuripe sofreu um ataque que afetou seriamente suas operações, exigindo que procedimentos fossem realizados manualmente e causando filas de embarcações.

Outro caso mais recente ocorreu em 2024, no Porto de São Francisco do Sul, onde um ataque de *ransomware* comprometeu mais de 880 mil documentos sensíveis, incluindo dados de contabilidade, contratos e operações. A operação foi parcialmente restaurada em menos de 24 horas, mas os sistemas de segurança foram restabelecidos gradualmente.

A abordagem ao risco cibernético na Resolução 53/2020 é particularmente inovadora, pois determina que o risco cibernético seja considerado parte integrante da gestão de riscos gerais em portos e terminais. Essa integração inclui a identificação sistemática de vulnerabilidades cibernéticas, a avaliação criteriosa de impactos na operação segura das instalações e a integração harmoniosa com outros tipos de riscos tradicionalmente considerados no ambiente portuário.

No entanto, apesar da abordagem inovadora da normativa, sabe-se que o Brasil ainda não despertou totalmente para a necessidade de investimentos robustos em cibersegurança, isso deixa muitos terminais expostos a riscos.

Após a análise das principais ameaças e vulnerabilidades presentes

no ambiente portuário e aduaneiro, torna-se fundamental avançar para a discussão de medidas capazes de prevenir, mitigar e responder a esses riscos. Nesse contexto, o próximo capítulo apresenta um conjunto de melhores práticas de segurança, reunindo orientações e procedimentos que podem ser adotados por autoridades, operadores e demais atores da comunidade portuária para fortalecer a proteção das instalações, das operações e das cadeias logísticas associadas ao comércio exterior.

8- Melhores práticas de segurança (forças)

Conforme definido na metodologia SWOT, adotada no presente Guia, as boas práticas correspondem às forças ("strengths") da análise. Entende-se por forças os aspectos internos e positivos de uma organização que lhe conferem vantagem competitiva. No caso em apreço, as boas práticas aqui elencadas são aquelas já adotadas e implementadas pelos terminais portuários, identificadas a partir das entrevistas e questionários conduzidos junto às instalações participantes.

Importa salientar que tais práticas não se confundem com o mero cumprimento de requisitos legais ou normativos. Pelo contrário, caracterizam-se por ir além das obrigações impostas pela legislação e regulamentação vigentes, traduzindo-se em ações voluntárias que visam ao aprimoramento contínuo da segurança. Assim, práticas que correspondam apenas ao atendimento estrito da lei não se enquadram, para fins deste capítulo, como "boas práticas".

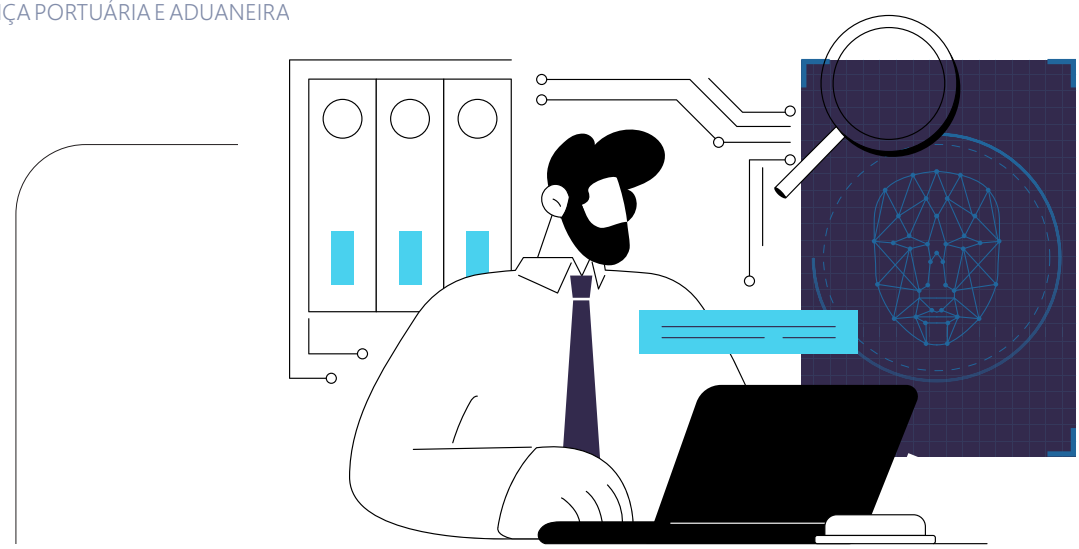
O presente capítulo apresenta, ainda, um quadro correlacionando cada boa prática com uma ou mais fraquezas ou ameaças identificadas no capítulo precedente. Tal correlação objetiva possibilitar que cada terminal portuário avalie a sua maior suscetibilidade frente a determinadas vulnerabilidades e, a partir disso, decida pela implementação de uma ou mais boas práticas. Ressalta- se que a aplicabilidade de cada prática dependerá das especificidades do terminal — tais como perfil de carga, porte, localização e demais características operacionais — sendo, portanto, decisão discricionária de cada instalação.

Cumpre destacar que diversos terminais e instalações portuárias compreendem em seu perímetro uma área alfandegada, sujeita às disposições da Portaria RFB nº 143/2022, bem como às respectivas normas complementares expedidas pela COANA.

Frequentemente, tais áreas estão submetidas a requisitos de segurança diferentes daqueles aplicáveis à área portuária como um todo. Nesse sentido, uma prática considerada adequada para a área portuária geral poderá não se revelar compatível com as exigências da área alfandegada.

A título exemplificativo, mencione-se que a Resolução nº 53 da CONPORTOS determina que o sistema de gravação de imagens do CFTV mantenha o registro por, no mínimo, 90 (noventa) dias. Já a Portaria RFB nº 143/2022 impõe que as imagens, dados e informações relativos à área alfandegada sejam armazenados por, no mínimo, 180 (cento e oitenta) dias. Desse modo, um procedimento de backup com prazo de retenção de 120 (cento e vinte) dias pode ser considerado uma boa prática, sob a ótica da Resolução nº 53 da CONPORTOS, mas não atenderá aos parâmetros exigidos para a área alfandegada, não configurando, portanto, boa prática nesse último caso.

Diante dessa realidade, foram registradas observações específicas ao longo da planilha de consolidação, assinalando as eventuais diferenças de abordagem entre as áreas alfandegadas e não alfandegadas, de modo a orientar as instalações quanto à adequada aplicação das práticas, considerando suas particularidades operacionais e normativas.



8.1 MELHORES PRÁTICAS NO COMBATE AO TERRORISMO E SABOTAGEM

1 Ações de inteligência voltadas ao combate do terrorismo.

▪ Adoção e implementação de estratégias integradas em colaboração com todos os órgãos públicos de segurança para prevenir e mitigar atividades terroristas nas infraestruturas portuárias e nos recintos aduaneiros. Exemplos: Participar de workshops e eventos que integram a comunidade portuária com órgãos de governo.

2 Investimento constante em equipamentos mais modernos, além do já determinado pela portaria COANA nº 80

▪ Aquisição de equipamentos além do já determinado pela portaria COANA nº 80, com objetivo de incorporar novas tecnologias, como sistemas avançados de monitoramento, automação e ferramentas de controle, a fim de garantir respostas mais eficazes contra o terrorismo nas instalações portuárias e em recintos aduaneiros. Um exemplo desses equipamentos seria a utilização de câmeras 4k. Apesar da utilização em algumas áreas alfandegadas ser obrigatória, a utilização em todo o terminal seria uma boa prática. Outro exemplo é a aplicação de IA específica e já existente, permitindo verificar padrões e anomalias nas imagens captadas pelas câmeras. Após essa identificação pela IA, um alerta é feito à equipe de segurança do terminal.

3 Realização de treinamentos e simulados constantes, em número superior aos exigidos pela norma, a fim de manter a equipe (de segurança e demais áreas) pronta para resposta a incidentes dessa natureza ou ainda que pelo menos um dos treinamentos e simulados obrigatórios aborde o tema do terrorismo.

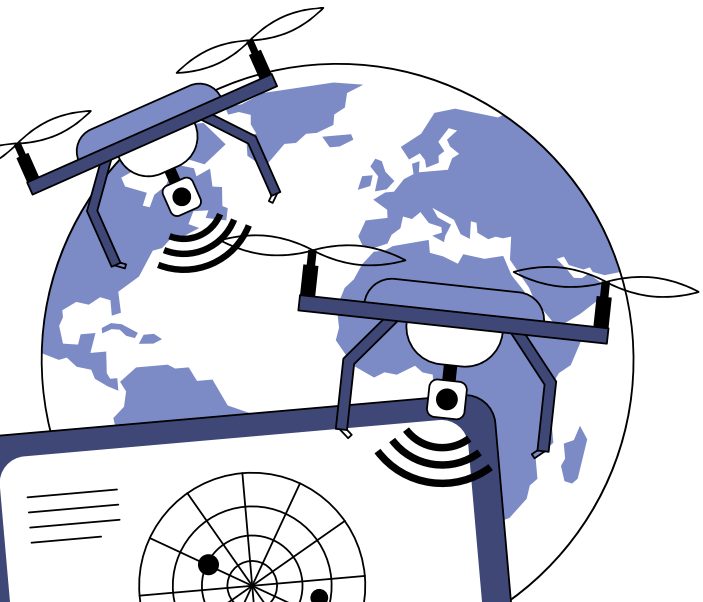
▪ Treinamentos e simulados destinados a preparar as equipes de segurança aduaneira para responder de forma eficaz a possíveis incidentes, reforçando a coordenação entre todos os envolvidos e permitindo a identificação e correção de falhas antes que ocorram situações reais. Exemplo: Participar de simulados e exercícios de outras instalações para promover integração, intercâmbio de conhecimentos e aprendizado mútuo.

4 Utilização de drones e detectores de metais.

▪ Equipamentos projetados para apoiar ações de combate ao terrorismo em infraestruturas portuárias e dos recintos aduaneiros, contribuindo para a proteção de instalações, a segurança de trabalhadores e usuários, bem como para a prevenção de ameaças.

5 Ronda perimetral por vigilantes.

▪ Uma equipe de vigilantes plenamente qualificada atua de forma preventiva por meio de rondas regulares em todo o perímetro da área portuária. Essas patrulhas são realizadas em intervalos estratégicos, com o objetivo de garantir a segurança contínua das instalações, preservar o patrimônio e assegurar a integridade das operações, prevenindo acessos indevidos e situações de risco..



6 Contratação de uma auditoria externa independente.

▪ A contratação de uma empresa externa tem como objetivo assegurar a conformidade com as normas de segurança, identificar ameaças e vulnerabilidades e implementar medidas preventivas eficazes. Com uma visão especializada e imparcial, a empresa contribui para um diagnóstico mais preciso e para a adequação dos procedimentos de segurança, alinhando-os às exigências regulatórias e às melhores práticas do setor.

7 Inspeções remotas (body cam) para os vigilantes no momento das rondas integradas ao sistema de controle de câmeras (CFTV).

▪ Essa ferramenta permite que os agentes de segurança realizem vistorias em tempo real, transmitindo imagens e áudio diretamente para a central de monitoramento. Tem como objetivo principal aumentar a cobertura e a eficácia da fiscalização, oferecendo uma visão em primeira pessoa das atividades, facilitando a tomada de decisões rápidas e a coordenação eficiente das operações, além de garantir maior transparência e segurança nas inspeções portuárias e aduaneiras.

8 Utilização de cancelas e catracas com dupla conferência.

▪ É uma medida de segurança que visa a reforçar o controle de acesso nas áreas portuárias. O sistema exige que os usuários passem por dois níveis de verificação, combinando a checagem de credenciais (como crachás, biometria ou códigos) e a inspeção física ou eletrônica de veículos e pessoas.

▪ Importante ressaltar que a dupla conferência (inclusive a biometria) já é obrigatória na área alfandegada, conforme disposto na legislação aduaneira.

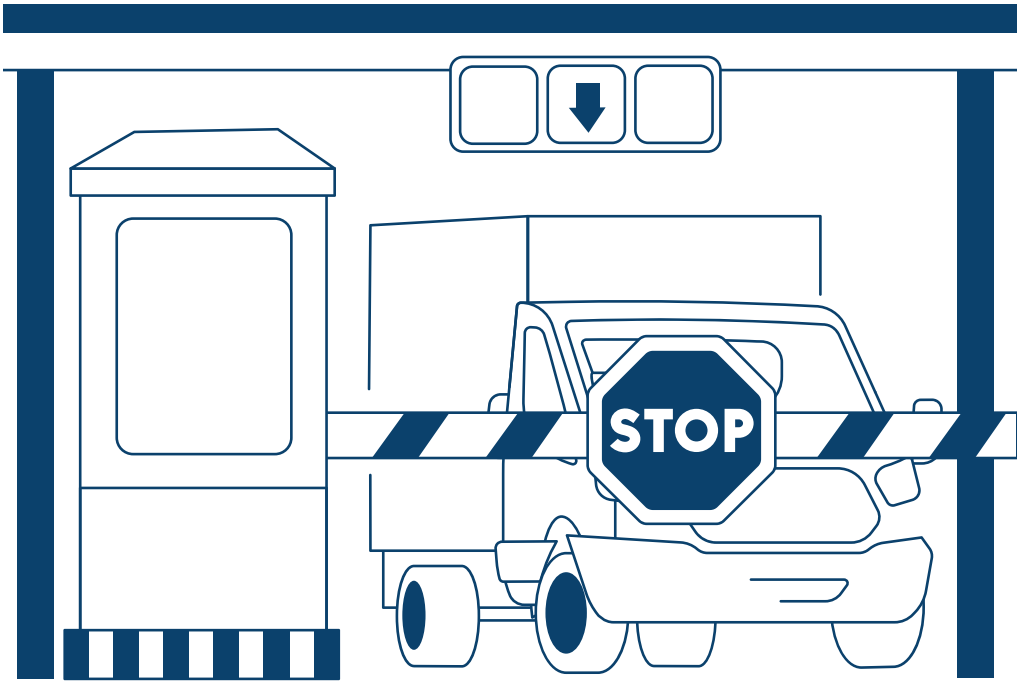
9 Utilização de drones, radares, câmeras térmicas, leitores faciais e detectores de metais como apoio às operações portuárias.

- Equipamentos projetados para apoiar ações de prevenção ao terrorismo em infraestruturas portuárias, contribuindo para a proteção de instalações, a segurança de trabalhadores e usuários, bem como para a prevenção de ameaças.

10 Utilizar a ISO 31000 como ferramenta para apoio e direcionamento das ações de inteligência, priorização e planejamento do mapeamento e ações de mitigação dos riscos.

- Utilização da ISO 31000 com o objetivo de estruturar processos a fim de identificar, analisar e avaliar ameaças potenciais, priorizando as mais críticas e apontar medidas de controle eficazes. Além disso, deve promover uma abordagem sistemática e contínua para a melhoria da segurança e da gestão de riscos nas estruturas avaliadas.

- Importante ressaltar que a ISO 31000 já é inerente à Resolução 53, dessa forma, é obrigatória. Mas é uma boa prática em termos de alfandegamento.

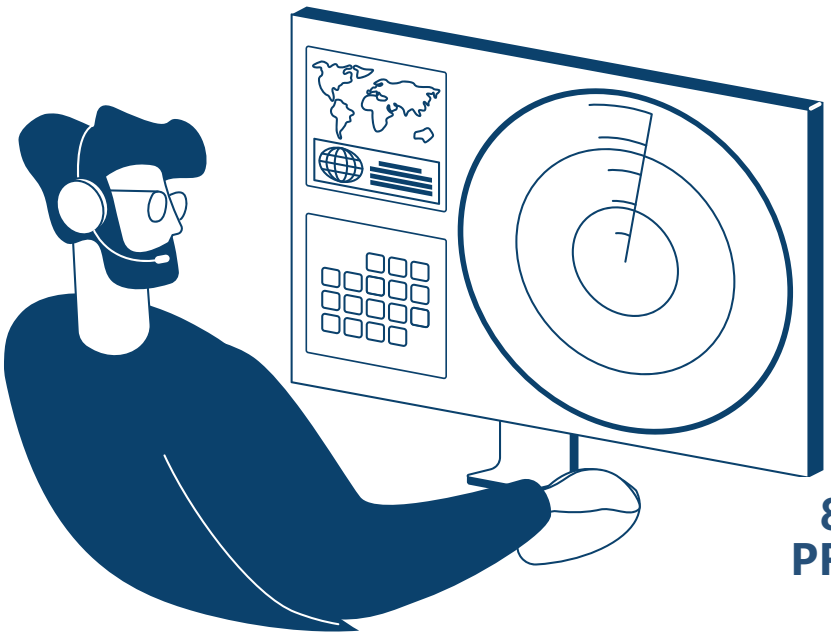


11 Realização de treinamentos e simulados, com o apoio das infraestruturas portuárias envolvidas, excedendo o número mínimo estipulado pelas normativas.

▪ Treinamentos e simulados, com o apoio das infraestruturas portuárias envolvidas, têm como objetivo preparar as equipes de segurança para responder de maneira eficaz a possíveis incidentes relacionados à temática terrorismo, fortalecendo a coordenação entre os participantes e permitindo a identificação e correção de falhas antes que se transformem em situações reais. Importante ressaltar que para ser boa prática deve-se exceder o número mínimo de treinamentos e simulados já definidos nas normativas afetas ao setor.

12 Realizar a gestão de pessoas e do clima organizacional

▪ Conforme visto no capítulo 7, a insatisfação do funcionário pode ser uma das principais origens da sabotagem, já que sentimentos de desvalorização, falta de reconhecimento ou sobrecarga de trabalho podem levá-lo a agir de forma prejudicial à organização. Nesse sentido, a boa prática de gestão de pessoas e o clima organizacional atuam de forma preventiva. Ao identificar sinais de desmotivação, oferecer canais de escuta e reconhecimento, além de promover um ambiente de trabalho saudável. Com isso, reduz-se significativamente o risco de que colaboradores insatisfeitos se tornem potenciais agentes de sabotagem.



8.2 MELHORES PRÁTICAS PARA LIDAR COM PASSAGEIROS CLANDESTINOS

13 Monitoramento com câmeras térmicas, radares de aproximação de embarcação, integrados ao CFTV do terminal.

▪ O monitoramento da escada do navio e da área marítima circundante é realizado por um sistema de CFTV que combina câmeras normais e térmicas, além de radares para detectar a aproximação de embarcações. Esse conjunto de tecnologias permite vigilância em tempo real, facilitando a identificação de movimentos suspeitos e prevenindo acessos não autorizados. A integração dessas soluções tecnológicas fortalece a segurança das operações portuárias e aprimora a capacidade de resposta a incidentes, garantindo uma proteção mais eficaz do perímetro.

14 Realização de vistoria agendada dos tripulantes e comprovação do que foi fiscalizado.

▪ A vistoria agendada dos tripulantes é um processo de inspeção periódica, previamente programada, com o objetivo de avaliar as condições de segurança, saúde e conformidade com as regulamentações vigentes. A comprovação da realização da fiscalização é efetuada por meio de registros oficiais, como relatórios detalhados e assinaturas, que certificam o cumprimento do cronograma e das diretrizes estabelecidas, garantindo a rastreabilidade e a transparência do procedimento.

15 Contato ativo com agências marítimas, para verificações prévias pela própria tripulação dos navios, ainda na área de fundeio.

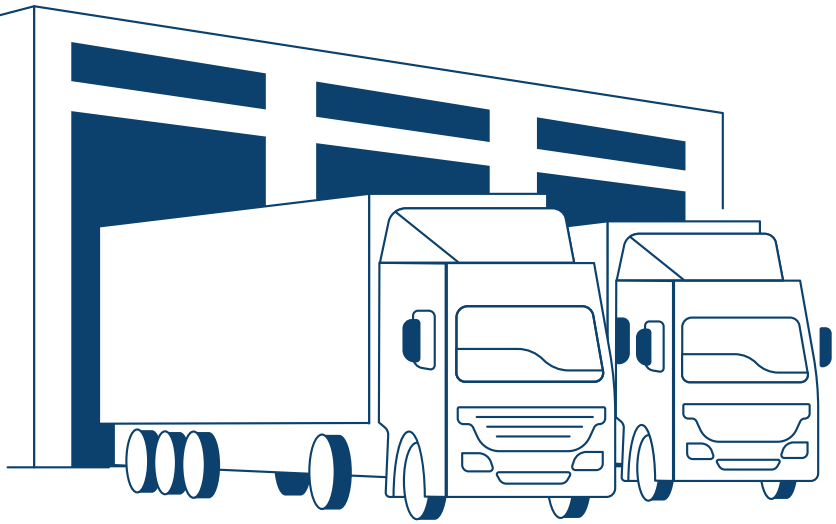
▪ O contato proativo com agências marítimas permite que a tripulação dos navios realize verificações preliminares enquanto ainda se encontra na área de fundeio. Essa prática garante a conformidade com as normas de segurança e possibilita a identificação antecipada de possíveis irregularidades. O intercâmbio eficaz de informações entre as agências e a tripulação fortalece a segurança das operações portuárias, contribuindo para a prevenção de incidentes antes da entrada no porto.

16 Interação com a Polícia Federal (NEPOM).

▪ A interação com a Polícia Federal, por meio do Núcleo Especial de Polícia Marítima (NEPOM), é fundamental para reforçar a segurança nas operações portuárias. Essa colaboração possibilita o intercâmbio de informações estratégicas e a coordenação de ações conjuntas, voltadas à prevenção e combate de crimes marítimos, como passageiros clandestinos. A sinergia entre as instituições não apenas aumenta a eficácia das operações de segurança, mas também contribui para a criação de um ambiente portuário mais seguro e protegido.

17 Acompanhamento de navios com origem em países onde há maior incidência de passageiros clandestinos.

▪ O acompanhamento de navios oriundos de países com alta incidência de clandestinos é uma estratégia crucial para fortalecer a segurança nas operações portuárias. Essa prática consiste na monitorização minuciosa das embarcações, com o objetivo de identificar e prevenir tentativas de acesso irregular. Ao manter a vigilância sobre essas origens, a empresa pode adotar medidas proativas para mitigar os riscos associados à imigração clandestina, garantindo, assim, a integridade e a segurança das atividades portuárias.



8.3 MELHORES PRÁTICAS NO COMBATE AO ROUBO, FURTO E EXTORSÃO

18 Veículos de cargas só podem acessar o porto por meio de agendamento.

- Todos os veículos de carga que acessam a infraestrutura portuária e aduaneira são previamente agendados e passam por um rigoroso sistema de controle de acesso. Esse processo assegura maior segurança e o cumprimento dos protocolos estabelecidos, garantindo uma operação portuária eficiente e alinhada às normas vigentes. Exemplo: Portos Rio no Rio de Janeiro pelo sistema SGAD.

- Exemplo: No agendamento, as informações podem não ser coerentes, como o mesmo veículo agendado em janelas com intervalos impossíveis de cumprir, denotando a necessidade de inspeção ou outro procedimento para garantir a segurança.

19 Conscientização de segurança sobre roubo de cargas com os colaboradores.

- É uma estratégia focada em educar e engajar os colaboradores sobre os riscos e as graves consequências do roubo de cargas. Por meio de treinamentos periódicos, campanhas de conscientização e uma comunicação interna eficiente, os funcionários são capacitados a identificar sinais de atividades suspeitas, entender as melhores práticas preventivas e seguir rigorosamente os protocolos de segurança.

20 Monitoramentos e rondas das áreas de armazenagens.

▪ Prática que consiste na vigilância contínua das áreas de armazenagem da infraestrutura portuária e alfandegária, utilizando sistemas avançados de monitoramento, como câmeras e sensores, complementados por rondas regulares das equipes de segurança. O principal objetivo é detectar e prevenir atividades suspeitas, assegurar a integridade das mercadorias e garantir a adesão rigorosa aos protocolos de segurança.

21 Monitoramento de contêineres.

▪ É uma estratégia que consiste no acompanhamento contínuo dos contêineres dentro da infraestrutura portuária e alfandegária, empregando tecnologias como câmeras, *scanners*, sensores e sistemas de rastreamento. O objetivo principal é assegurar a segurança das cargas, prevenindo roubos, violações e movimentações não autorizadas, além de garantir que os contêineres cumpram os procedimentos de integridade estabelecidos. Exemplo: Posicionamento dos contêineres nas pilhas com as portas em única direção, de modo que exista pelo menos uma câmera mostrando todas as portas do nível inferior, capaz de detectar qualquer pessoa em circulação entre as pilhas.

22 Realização do espelhamento/compartilhamento do sistema de rastreamento - REDEX com o terminal.

▪ Implementação do espelhamento e compartilhamento do sistema de rastreamento REDEX com o terminal portuário, permitindo uma integração eficaz entre as operações aduaneiras e as atividades do terminal. Essa prática visa a melhorar a visibilidade e o controle sobre a movimentação de cargas, facilitando a identificação de irregularidades, otimização dos processos logísticos e fortalecimento da segurança nas operações portuárias. Exemplo: O acompanhamento do percurso dos caminhões entre o REDEX e o Terminal pode identificar desvio de rota e controlar o fluxo de chegada por meio das janelas de agendamento.

23 Utilização de sistema específico que contenha informações do veículo e motorista.

- A utilização do sistema específico que se refere à adoção de uma plataforma a qual armazena e gerencia informações abrangentes sobre veículos e motoristas que acessam o porto. Esse sistema fornece dados essenciais, como identificação do motorista, tipo de veículo e histórico de acesso, possibilitando um controle rigoroso e eficiente das operações portuárias. A implementação desse sistema aprimora a segurança, dá agilidade e organização no gerenciamento de entradas e saídas, além de garantir a conformidade com os protocolos de segurança estabelecidos.

24 Utilização de sistema de OCR nas balanças de pesagem sem intervenção humana na pesagem.

- A utilização de sistema de Reconhecimento Óptico de Caracteres (OCR) nas balanças, isso possibilita a leitura automática de dados sem intervenção humana. O principal objetivo é aumentar a eficiência e a precisão na coleta de informações sobre o peso das cargas, reduzindo erros e agilizando todo o processo de pesagem. Essa inovação não apenas otimiza as operações logísticas, mas também garante um controle mais rigoroso sobre as cargas, promovendo a integridade dos dados.

- Importante ressaltar que essa utilização já é obrigatória em recintos alfandegados.

25 Tratamento diferenciado para as empresas transportadoras que possuam monitoramento de cargas.

- Tratamento diferenciado para as empresas transportadoras que possuam sistema de monitoramento de cargas no modal rodoviário (Exemplo: utilização de *fast lanes* para tais empresas no acesso ao terminal).

- O sistema de monitoramento dessas empresas pode ser, por exemplo, uma plataforma de gestão integrada que visa ao monitoramento e controle de cargas, tendo como objetivo otimizar as operações logísticas, oferecendo funcionalidades que incluem rastreamento de caminhões, gerenciamento de documentos e coordenação da movimentação de cargas. Com essa ferramenta, é possível aumentar a eficiência das operações, garantir a segurança das mercadorias e melhorar a transparência no fluxo de informações entre todos os envolvidos na cadeia logística.

26 Realização de treinamento sobre como agir em casos de extorsão, quando são abordadas e a quem reportar nesses casos.

- Implementação de treinamentos específicos para capacitar as equipes a lidarem com situações de extorsão. O programa abrange orientações sobre como identificar sinais de extorsão, procedimentos adequados para proteger a integridade pessoal e da operação, e diretrizes claras sobre a quem reportar esses incidentes. Essa prática busca fortalecer a segurança, garantir respostas eficazes e proteger os colaboradores e as operações portuárias.

27 Fortalecimento e divulgação do canal de denúncias

▪ O fortalecimento e a divulgação do canal de denúncias buscam aprimorar e ampliar a visibilidade do canal de denúncias da Companhia, oferecendo um meio seguro e confidencial para que colaboradores e terceiros possam relatar irregularidades. O fortalecimento do canal garante que todas as denúncias sejam tratadas com seriedade e investigadas de acordo com a sua classificação. Deve haver treinamento para que o colaborador saiba como agir e o que fazer nos casos em que receba esse tipo de abordagem. A extorsão é crime e deve ser reportado às autoridades policiais.

28 Atuação conjunta dos setores de ouvidoria e *compliance* para acompanhar e tratar denúncias de eventuais casos de extorsão.

▪ A atuação conjunta dos setores de ouvidoria e *compliance* envolve a colaboração entre esses departamentos para monitorar e tratar denúncias relacionadas a possíveis casos de extorsão. A parceria entre ouvidoria e *compliance* assegura uma análise ágil e minuciosa das denúncias, garantindo que todas as alegações sejam investigadas de forma rigorosa e que ações corretivas sejam implementadas rapidamente. Essa abordagem conjunta fortalece a integridade e a transparência nas operações da Companhia, reforçando o compromisso com a ética e a governança.

29 Possuir uma política corporativa sobre antiextorsão.

▪ A política corporativa de antiextorsão define diretrizes claras para prevenir, identificar e combater práticas de extorsão na Companhia. Essa política estabelece padrões de conduta para todos os colaboradores e parceiros, reforçando o compromisso da organização com a ética e a integridade em todas as suas operações. Além de proteger a empresa contra ameaças externas, a política assegura que quaisquer casos de extorsão sejam tratados com rigor e transparência, promovendo um ambiente de negócios seguro e alinhado às melhores práticas de governança.

30 Implementar as ações da Política de Transação com Partes Relacionadas, baseada na Lei Federal 13.303/16.

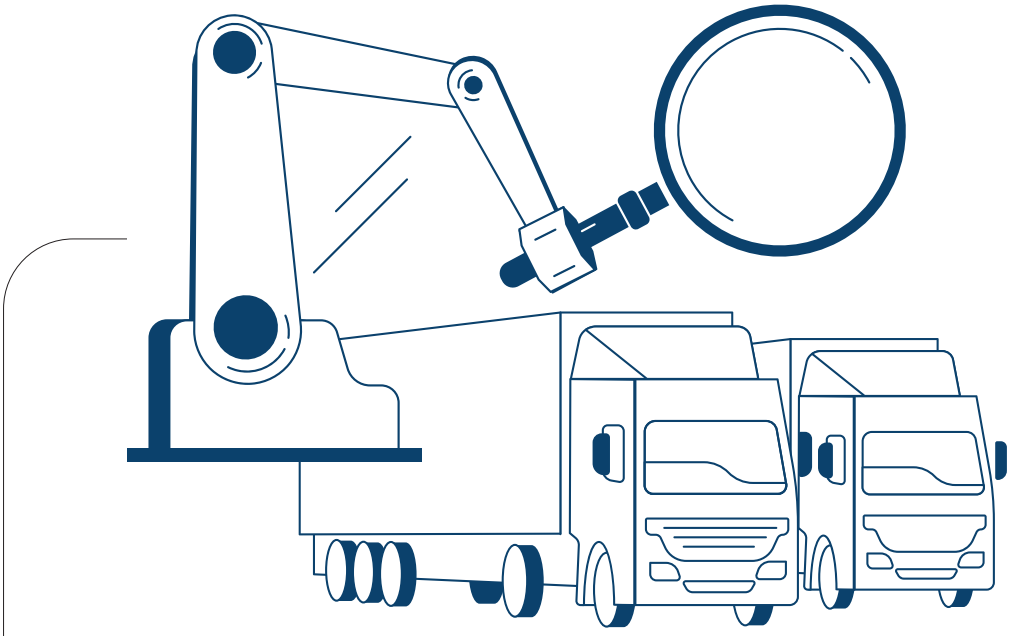
▪ A implementação da Política de Transação com Partes Relacionadas refere-se à aplicação das diretrizes estabelecidas pela Lei Federal 13.303/16. Essa prática visa a assegurar transparência e conformidade nas transações entre a empresa e seus parceiros, prevenindo conflitos de interesse e garantindo que todas as operações sejam realizadas de maneira ética e responsável. A política reforça a integridade nas relações comerciais, alinhando as práticas da empresa às exigências legais e aos princípios de governança corporativa.

31 Vigilantes juntos (trabalho em dupla) e câmeras na fiscalização do contêiner.

▪ A fiscalização de contêineres com vigilância em dupla e câmeras envolvem a atuação de duas equipes de vigilantes trabalhando em conjunto, apoiadas por um sistema de câmeras de monitoramento, para garantir a segurança e a integridade dos contêineres. Essa abordagem colaborativa melhora a eficácia na detecção de atividades suspeitas, inibe a possibilidade de recebimento de valores monetários para facilitar a fiscalização e possibilita uma resposta rápida a incidentes, assegurando um ambiente operacional seguro e protegido nas instalações portuárias e áreas alfandegadas.

32 Disponibilizar canal de denúncias com ligação gratuita, cujas denúncias são recebidas e triadas por instituição independente, ligada apenas ao setor de *compliance*.

▪ O canal de denúncias com ligação gratuita: essa prática oferece um canal de denúncias acessível via uma linha gratuita, onde as denúncias são recebidas e triadas por uma instituição independente, exclusivamente ligada ao setor de *compliance*. O objetivo é assegurar que todas as denúncias sejam tratadas de maneira confidencial e imparcial, promovendo um ambiente de integridade e transparência na organização, e incentivando a colaboração de todos os funcionários na identificação de irregularidades.



8.4 MELHORES PRÁTICAS NO COMBATE AO TRÁFICO, DESCAMINHO E CONTRABANDO

33 Colaboração em ações de inteligência voltadas ao combate do tráfico.

- As ações de inteligência para o combate ao tráfico em portos e áreas aduaneiras focam na coleta, análise e compartilhamento de informações estratégicas, com o objetivo de desmantelar redes criminosas de forma eficiente. Essas atividades incluem monitoramento constante de comportamentos suspeitos e o uso de tecnologias avançadas, como sistemas de vigilância, softwares de análise preditiva e ferramentas de rastreamento de cargas.

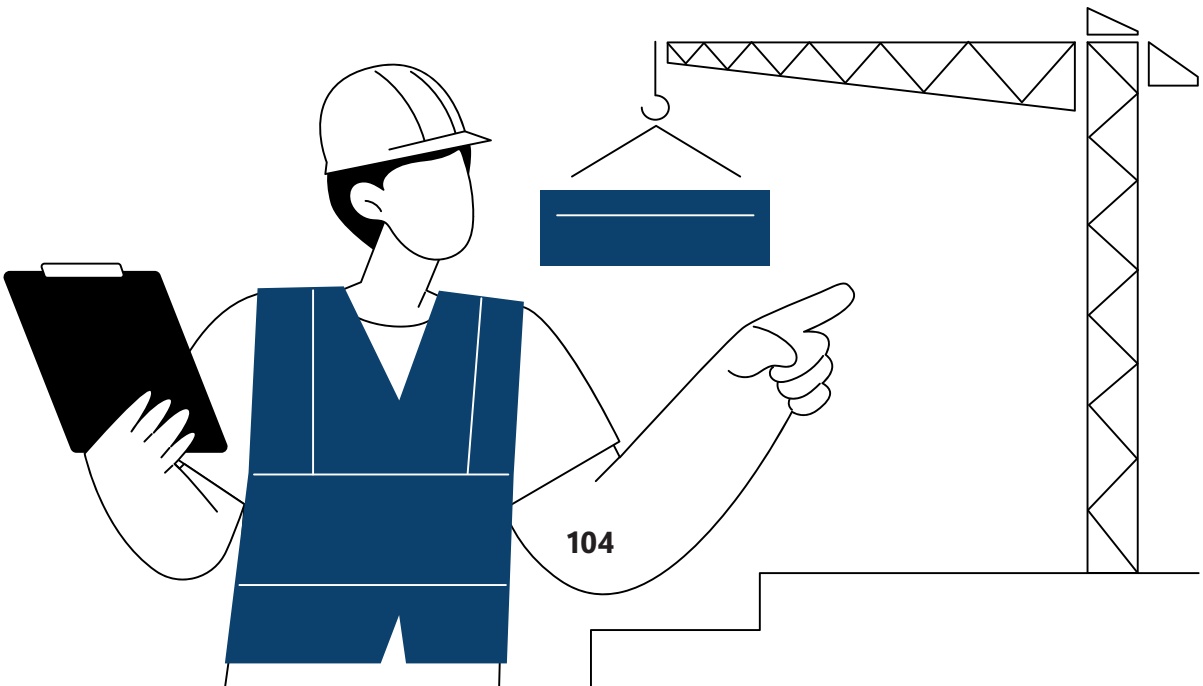
- Entre as estratégias, destaca-se a colaboração estreita entre infraestruturas portuárias e forças de segurança, bem como a realização de reuniões periódicas para antecipar atividades ilícitas, identificar rotas de contrabando e padrões operacionais. Essas medidas aumentam a precisão e a agilidade nas operações de fiscalização e apreensão. Adicionalmente, a criação de grupos de trabalho ou comitês especializados pode agilizar e fortalecer as ações de inteligência no combate ao tráfico.

34 Inspeções remotas (body cam) integradas ao sistema de controle de câmeras (CFTV) que, de maneira “on-line”, o operador conversa com o time de segurança, gravando a filmagem e fazendo áudio em casos suspeitos (em todas as rondas).

▪ As inspeções remotas, utilizando body cams integradas ao sistema de CFTV, capacitam os operadores a monitorarem as rondas de segurança em tempo real. Durante as patrulhas, o operador pode se comunicar diretamente com a equipe, registrando simultaneamente imagens e áudio em situações suspeitas. Esse sistema não apenas assegura um registro mais preciso das ocorrências, mas também agiliza a tomada de decisões e aumenta a transparência e a eficiência das operações de segurança, contribuindo para um ambiente mais seguro.

35 Treinamento de prevenção ao uso e abuso de drogas.

▪ O treinamento de prevenção ao uso e abuso de drogas é uma iniciativa crucial e está alinhado à política de RH para capacitar profissionais de segurança e colaboradores em portos e áreas aduaneiras. Esse programa abrange os riscos associados ao consumo de substâncias ilícitas, estratégias para identificar comportamentos indicativos de uso de drogas e técnicas de intervenção eficazes. Além disso, ele promove a conscientização sobre políticas de prevenção e recursos de apoio disponíveis, visando a estabelecer um ambiente de trabalho mais seguro e saudável, ao mesmo tempo em que fortalece a cultura de responsabilidade e bem-estar entre os colaboradores.



36 Colaboração com órgãos de segurança, outros terminais e portos, e intensificação do controle de acesso de prestadores de serviço ao navio, monitoramento de câmeras no contrabordo.

▪ A intensificação do controle de acesso para prestadores de serviço ao navio é uma estratégia essencial para garantir a segurança nas operações portuárias. Essa abordagem envolve a verificação rigorosa de credenciais e o monitoramento contínuo por meio de câmeras de vigilância posicionadas no contrabordo. O acompanhamento em tempo real assegura que somente o pessoal autorizado possa acessar as embarcações, reduzindo significativamente os riscos de contrabando e atividades ilícitas, e contribuindo para um ambiente mais seguro e protegido nas operações portuárias e alfandegárias.

37 Utilização, como referência da certificação OEA, a aplicação da técnica de inspeção de caminhões e contêineres denominada 7/17 pontos, baseada em Gestão de Riscos de Segurança da Cadeia Logística.

▪ Utilizar como referência as técnicas de vistoria 7/17 pontos, conforme preconiza o Programa OEA (Operador Econômico Autorizado), no momento da entrada do caminhão no Terminal, com o objetivo de assegurar a conformidade com os padrões internacionais de segurança do comércio exterior. Esse procedimento avalia rigorosamente a integridade das cargas e a documentação envolvida, garantindo que a carga, o contêiner e o veículo não tenham sofrido violação e/ou contaminação com a inclusão de drogas durante o percurso até o Terminal. Com isso, promove maior eficiência operacional e aumenta a confiabilidade nas transações comerciais, fortalecendo a segurança e a conformidade nas operações portuárias e alfandegárias.

38 Reanálise de imagem de scanner.

▪ A reanálise de imagens de scanner é um procedimento fundamental que envolve a revisão minuciosa das imagens obtidas durante as inspeções de carga. Realizada por especialistas treinados e em áreas externas à infraestrutura portuária, essa prática tem como objetivo identificar anomalias ou riscos que possam ter passado despercebidos na análise inicial. A reanálise aumenta a precisão na detecção de materiais ilícitos e fortalece a segurança nas operações portuárias e alfandegárias, garantindo um controle rigoroso sobre as mercadorias que entram e saem das instalações. Exemplo: Fora ou mesmo dentro do Terminal, uma equipe técnica adicional fica em local distante do scanner, acessando um equipamento independente, capaz de replicar as imagens geradas no scanner, constituindo uma análise redundante do conteúdo do contêiner por duas equipes sem contato direto.

39 Sistema próprio de análise de riscos, confrontando informações como: origem, destino, nacionalidade da tripulação.

▪ O sistema próprio de análise de riscos é uma ferramenta projetada para avaliar e confrontar informações cruciais relacionadas à segurança portuária. Ele analisa dados como a origem e o destino das cargas, bem como a nacionalidade da tripulação, permitindo a identificação de padrões e a detecção de potenciais ameaças. Essa abordagem proativa não apenas facilita a tomada de decisões informadas, mas também otimiza a implementação de medidas de mitigação, contribuindo significativamente para a segurança e integridade das operações portuárias.

40 Complementar a inspeção feita com scanner e CFTV com vistoria física.

▪ A combinação de inspeção por scanner e CFTV com vistoria física reforça a segurança e eficácia no controle de cargas. Enquanto o scanner e o CFTV oferecem uma análise inicial rápida e abrangente, a vistoria física permite identificar detalhes que podem passar despercebidos pelos sistemas eletrônicos, garantindo maior precisão na detecção de irregularidades. Essa prática aumenta a confiabilidade das inspeções, reduzindo riscos de contrabando e violações, e assegura a integridade das operações portuárias. Exemplo: O scanner e o CFTV não detectam um lacre rompido, uma avaria nas portas do contêiner, uma falsificação no número do lacre ou do próprio contêiner, entre outros.

41 Monitoramento em tempo real das rondas por meio de tecnologia.

▪ Adotar tecnologia para o monitoramento em tempo real das rondas, utilizando dispositivos móveis e GPS. Essa abordagem permite acompanhamento contínuo, rápida identificação de incidentes, geração automática de relatórios, melhora a comunicação e agiliza a resposta a emergências.

42 Utilização da plataforma (app) para realizar gestão de riscos nas operações portuárias.

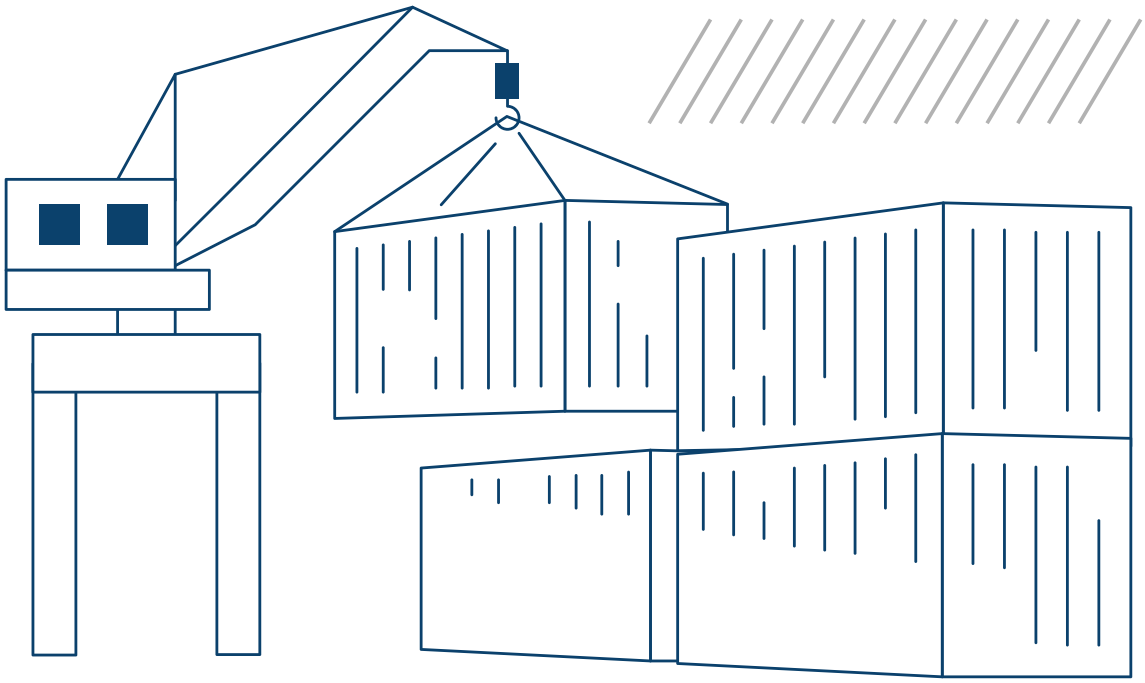
▪ É uma ferramenta avançada para a gestão de riscos nas operações portuárias. Essa plataforma fornece análises detalhadas e relatórios sobre os riscos associados a portos e terminais, com base em dados globais e critérios de segurança reconhecidos internacionalmente. Essa solução permite tomar decisões mais assertivas, identificar vulnerabilidades e adotar medidas preventivas de forma proativa, melhorando a segurança e a eficiência das operações portuárias.

43 Realização de simulações de invasão e uso de imagens e alarmes falsos para testes da eficácia dos controles e da capacidade de reação dos vigilantes em uma quantidade superior ao que a lei exige.

▪ Conduzir simulações de invasão com imagens e alarmes falsos para avaliar a eficácia dos sistemas de segurança e a capacidade de resposta dos vigilantes, realizando-as em frequência superior ao exigido por lei. Essa abordagem assegura uma preparação mais robusta e contribui para a melhoria contínua dos protocolos de segurança.

44 Escaneamento de 100% das cargas que foram identificadas como de risco, segundo as diretrizes da autoridade aduaneira, ou mecanismos como denúncias e gerenciamento de riscos.

▪ Uma vez que é quase impossível o escaneamento de 100% dos contêineres, até porque pode-se prejudicar o fluxo de comércio lícito, uma boa prática tem sido a implementação de um gerenciamento de risco, inclusive com a participação de fiscais e agentes policiais colaboradores, com base em dados e informações das quais essas autoridades têm conhecimento. A partir de então é realizado o escaneamento de 100% das cargas que foram identificadas como de risco segundo as diretrizes da autoridade aduaneira, ou mecanismos como denúncias e gerenciamento de riscos.



8.5 MELHORES PRÁTICAS NO COMBATE À ESPIONAGEM INDUSTRIAL

45 Verificar a origem dos equipamentos adquiridos para os terminais e áreas alfandegadas

- Realizar uma verificação rigorosa da origem e da procedência de todos os materiais adquiridos, especialmente os de origem estrangeira, para garantir que não contenham dispositivos ou *softwares* que possam comprometer a segurança do terminal.

- Estabelecer protocolos de auditoria e testes de segurança em equipamentos antes de sua instalação, assegurando que não sejam utilizados para atividades de espionagem industrial.

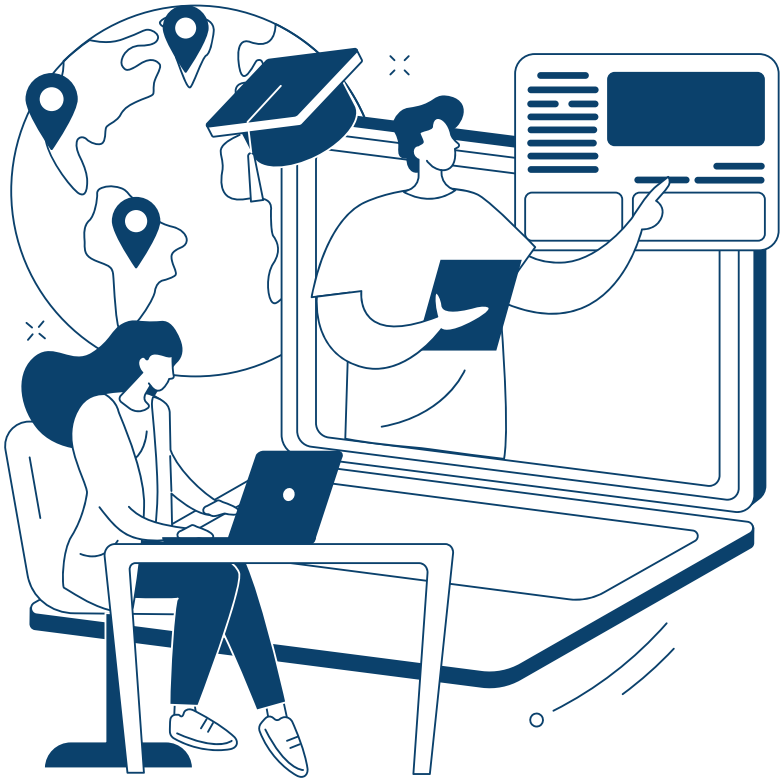
46 Política de Segurança da Informação

- A Política de Segurança da Informação consiste em um conjunto abrangente de diretrizes e práticas projetadas para proteger os ativos informacionais da organização. Ela estabelece claramente as responsabilidades dos colaboradores, os procedimentos para o manejo de dados e as medidas necessárias para mitigar ameaças cibernéticas e prevenir vazamentos de informações. O objetivo central dessa política é assegurar a confidencialidade, integridade e disponibilidade dos dados, promovendo uma cultura de segurança alinhada com as regulamentações vigentes. Além disso, a política atua como um guia para a resposta a incidentes e para a melhoria contínua das práticas de segurança da informação dentro da empresa.

47 Criar e manter um Comitê de Gestão de Riscos.

▪ Instituir um Comitê de Gestão de Riscos com membros de diferentes áreas para assegurar uma abordagem integrada na identificação, avaliação e mitigação de riscos. O comitê deve formular políticas, monitorar continuamente os riscos, implementar ações preventivas e corretivas e comunicar os riscos à alta administração. Reuniões periódicas são essenciais para revisar estratégias, acompanhar indicadores e garantir conformidade com regulamentações, promovendo uma cultura sólida de gestão de riscos.

▪ Importante ressaltar que esse item já é obrigatório para quem é OEA.



8.6 MELHORES PRÁTICAS PARA MITIGAR TREINAMENTOS INADEQUADOS

48 Planejamento Estruturado de Treinamentos

▪ Os treinamentos de pessoal (além dos já exigidos por normativas) devem garantir que sejam contemplados todos os níveis hierárquicos, desde a operação até a alta gestão. Além disso, deve-se atualizar periodicamente o conteúdo, incorporando novos riscos, tecnologias e lições aprendidas de incidentes.

49 Instrutores Qualificados e Conteúdo Padronizado

▪ Importante selecionar instrutores certificados e com experiência prática em segurança portuária, e utilizar manuais, protocolos e simulações padronizados, garantindo consistência entre diferentes turmas.

8.7 MELHORES PRÁTICAS NO COMBATE AO CIBERATAQUE

50. Aplicar NIST e ISO/IEC FAMÍLIA 27000

▪ Adotar práticas consolidadas de segurança da informação, reconhecidas pela Organização Marítima Internacional na MSC-FAL.1/Circ.3/Rev.3 - 4 April 2025, que são diretrizes reconhecidas internacionalmente, com foco na proteção contra ameaças cibernéticas, no gerenciamento eficiente da infraestrutura de TI e na manutenção da continuidade dos serviços como a NIST CSF e as normas da Família ISO 27000. O NIST CSF oferece um *framework* abrangente que orienta a avaliação e mitigação de riscos à segurança cibernética, apresentando diretrizes práticas para proteger sistemas e dados. A norma principal, ISO 27001, define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), enquanto outras normas da família fornecem diretrizes e práticas recomendadas para diferentes aspectos da segurança da informação. Dentre elas, a ISO/IEC 27002 é um padrão internacional que fornece diretrizes para a seleção, implementação e gestão de controles de segurança da informação. A gestão de tecnologia da informação deve ser conduzida com base em padrões de boas práticas que abrangem desde a governança até a operação e suporte técnico. A rede de TI dedicada à segurança empresarial, quando segregada das demais redes organizacionais, garante maior controle e proteção. A implementação de um sistema de autenticação multifatorial, que exige a combinação de diferentes métodos de verificação, contribui para garantir o acesso seguro aos serviços digitais. A combinação dessas normas capacita as organizações a desenvolverem e manterem políticas de segurança robustas, assegurando a proteção eficaz das informações e a conformidade com regulamentações relevantes.

51 Implementação das ISO 22301 – Gestão de Continuidade dos Negócios; ISO 31000 – Os Princípios e Diretrizes da Gestão de Riscos; COBIT – *Control Objectives for Information and Related Technology.*

▪ A implementação das normas ISO 22301, ISO 31000 e COBIT é crucial para aprimorar a gestão de riscos e garantir a continuidade dos negócios na organização. A ISO 22301 estabelece um framework robusto para a Gestão de Continuidade dos Negócios, assegurando que a empresa mantenha suas operações essenciais em face de eventos disruptivos. A ISO 31000 fornece princípios e diretrizes claras para a Gestão de Riscos, promovendo uma abordagem sistemática na identificação, avaliação e mitigação de riscos. Por sua vez, o COBIT oferece melhores práticas e objetivos de controle para a governança e o gerenciamento de tecnologia da informação, garantindo que os ativos de TI estejam alinhados às metas estratégicas da organização.

52 Possuir equipe corporativa de TI que cuida de segurança cibernética.

▪ A constituição de uma equipe corporativa de TI especializada em segurança cibernética é crucial para a proteção da organização contra ameaças digitais. Essa equipe desempenha um papel fundamental na monitorização, identificação e resposta a incidentes de segurança, além de desenvolver e implementar políticas e práticas robustas de proteção de dados. Com vasta experiência em tecnologias de segurança, os profissionais também conduzem treinamentos e campanhas de conscientização para os colaboradores, promovendo uma cultura de segurança organizacional. A atuação proativa dessa equipe não apenas reforça a integridade dos sistemas e a proteção das informações sensíveis, mas também assegura a continuidade dos negócios em um ambiente digital seguro e resiliente.

53 Investir em curso de pós-graduação na área cibernética para colaboradores e capacitação da equipe em segurança da informação.

▪ A empresa investe em cursos de pós-graduação na área cibernética para seus colaboradores, com o objetivo de aprimorar suas competências e conhecimentos em segurança da informação. Essa iniciativa reflete o compromisso da organização com o desenvolvimento profissional de sua equipe, capacitando-os a enfrentar desafios emergentes no campo da cibersegurança. A capacitação da equipe em segurança da informação é um processo fundamental que tem como objetivo aprimorar as habilidades e conhecimentos dos colaboradores na proteção de dados e ativos da organização. Esse processo envolve treinamentos regulares sobre práticas de segurança, reconhecimento de ameaças cibernéticas e estratégias de resposta a incidentes. Ao investir em formação contínua, a empresa garante que sua equipe esteja bem-informada e preparada para enfrentar os desafios do ambiente digital.

54 Conscientizar os usuários sobre as boas práticas de segurança (senhas fortes, abertura de *links* e *e-mails* suspeitos.

▪ A conscientização dos usuários sobre boas práticas de segurança é fundamental para salvaguardar a organização contra ameaças cibernéticas. Essa iniciativa abrange orientações para a criação de senhas fortes, desencorajando o uso de combinações previsíveis e enfatizando a importância da troca regular de senhas. Além disso, é vital alertar os usuários sobre os perigos de abrir *links* e *e-mails* suspeitos, que podem resultar em ataques de *phishing* ou infecções por *malware*.

55 *Scan* de vulnerabilidade realizado por consultoria externa.

▪ A realização de um *scan* de vulnerabilidade por uma consultoria externa é uma prática estratégica essencial para identificar e avaliar fraquezas potenciais na segurança da infraestrutura de TI da organização. Esse processo envolve uma análise minuciosa de sistemas, redes e aplicações, com o objetivo de detectar vulnerabilidades que possam ser exploradas por agentes maliciosos. Ao contar com a experiência de profissionais especializados, a empresa obtém uma avaliação imparcial e abrangente de suas fraquezas, permitindo a implementação de medidas corretivas eficazes.

56 Testes periódicos de *phishing*.

▪ Testes periódicos de *phishing* são fundamentais para avaliar a conscientização e a resiliência dos colaboradores frente a tentativas de fraudes cibernéticas. Essas simulações envolvem o envio de *e-mails* que imitam ataques de *phishing*, permitindo à organização identificar vulnerabilidades e analisar a capacidade de resposta dos funcionários. Ao realizar esses testes de forma regular, a empresa não só reforça a formação em segurança da informação, mas também corrige falhas de conscientização, promovendo uma cultura de segurança proativa. Essa abordagem minimiza o risco de ataques reais e protege os dados sensíveis da organização, fortalecendo sua postura de segurança cibernética.

57 Equipe de especialistas dedicados à cibersegurança, treinados nas tecnologias implementadas.

▪ A equipe de cibersegurança é composta por profissionais qualificados e treinados nas tecnologias utilizadas pela organização. Eles são responsáveis por monitorar, identificar e responder a ameaças cibernéticas, protegendo os ativos digitais. O treinamento contínuo garante que estejam atualizados com as tendências e técnicas de segurança, possibilitando uma abordagem eficaz na mitigação de riscos. Essa prática fortalece a resiliência da organização e promove uma cultura de segurança alinhada às melhores práticas corporativas. Diferente do exposto no item 49, nesse caso temos uma equipe dedicada a esse ponto.

58 Treinamento sobre a temática cibersegurança.

▪ O treinamento em cibersegurança é uma iniciativa essencial para equipar os colaboradores com conhecimentos sobre práticas seguras no ambiente digital. Esse programa é abrangente, com temas como identificação de ameaças, proteção de dados, uso seguro de redes e prevenção de ataques cibernéticos. Ao elevar a conscientização sobre riscos e melhores práticas, o treinamento fomenta uma cultura de segurança robusta dentro da organização, reduzindo vulnerabilidades e reforçando a proteção das informações corporativas. Com uma equipe bem treinada, a empresa se torna mais resiliente contra incidentes cibernéticos, promovendo um ambiente de trabalho seguro e confiável.

59 Estudo de avaliação de risco sobre cibersegurança.

▪ O estudo de avaliação de risco em cibersegurança consiste em uma análise abrangente que identifica, avalia e prioriza os riscos relacionados à segurança da informação na organização. Esse processo inclui a revisão minuciosa de sistemas, redes e procedimentos atuais, visando a detectar vulnerabilidades e ameaças potenciais. A partir dos resultados obtidos, são elaboradas estratégias e recomendações específicas para mitigar os riscos, reforçando a proteção dos dados e assegurando a conformidade com as normas de segurança. Essa avaliação é essencial para fortalecer a resiliência cibernética da empresa e salvaguardar seus ativos digitais. De forma adicional, além do já avaliado pelo EAR da Resolução 53.

60 Integração de novos colaboradores com foco em cibersegurança e divulgação da PSI, com emissão de termo de conhecimento.

▪ A integração de novos colaboradores com foco em cibersegurança é um processo crucial que educa os recém-contratados sobre as políticas de segurança da informação (PSI) da organização. Nesse processo, são apresentados princípios e práticas fundamentais de segurança, enfatizando a importância da proteção de dados e da prevenção de ameaças cibernéticas. Os novos colaboradores também assinam um termo de conhecimento, atestando sua compreensão e compromisso em aderir às diretrizes de segurança estabelecidas. Essa abordagem assegura que todos os funcionários estejam alinhados com a cultura de segurança da organização desde o início de sua jornada profissional.

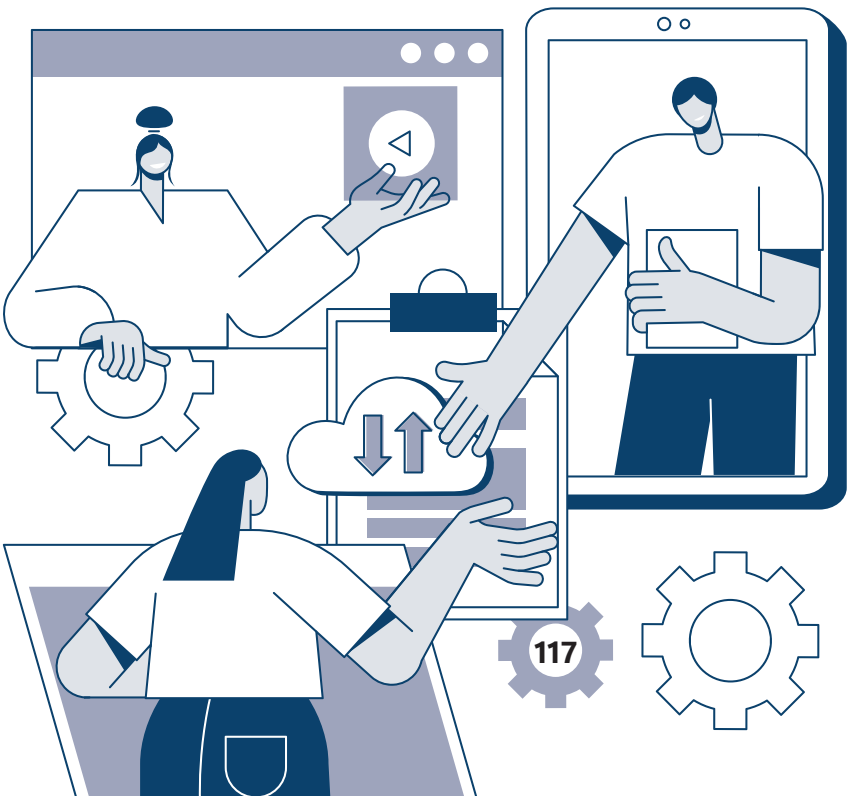
61 Servidor de AD.

▪ O servidor de *Active Directory* (AD) é um componente crítico em ambientes corporativos, responsável por gerenciar identidades e recursos de rede de forma centralizada. Ele fornece uma estrutura robusta para autenticação e autorização de usuários e dispositivos, permitindo um controle preciso sobre o acesso a informações e serviços da organização. Com o AD, é possível implementar políticas de segurança, gerenciar grupos de usuários e definir permissões de acesso de maneira eficaz. Além disso, o servidor de AD simplifica a administração da rede, assegurando que as operações sejam conduzidas de maneira segura e organizada, o que é fundamental para manter a integridade e a proteção dos dados corporativos.

62 Realizar teste de penetrações nos sistemas.

▪ Uma empresa especializada é contratada para conduzir ataques simulados no sistema de maneira regular, visando a identificar vulnerabilidades e avaliar a eficácia das defesas cibernéticas. Esses testes não apenas ajudam a fortalecer a segurança do sistema, mas também fornecem *insights* valiosos que permitem ajustes e melhorias contínuas na proteção contra ameaças reais.

▪ O teste é uma simulação de ação ofensiva externa, diferente do item 52 que é o escaneamento de vulnerabilidades responsável por analisar a rede e superfície externa.



63 Investimento em *backup* automático e imediatamente (minutos ou horas de perda).

▪ O investimento em *backup* automático é fundamental para proteger os dados da organização e garantir uma recuperação rápida, em casos de incidentes. Com *backups* realizados em intervalos regulares, a perda de informações é reduzida a apenas alguns minutos ou horas, o que assegura a continuidade das operações e a integridade dos dados. Essa abordagem não só aumenta a segurança, mas também proporciona tranquilidade à organização, diante de falhas ou ataques cibernéticos.

64 Espelhamento de servidores para garantir a segurança das operações.

▪ O espelhamento de servidores é uma estratégia fundamental para assegurar a continuidade e segurança das operações da organização. Essa prática consiste na duplicação em tempo real de dados e aplicações em servidores secundários, garantindo que, em caso de falha ou ataque ao servidor principal, as operações possam ser restauradas rapidamente e sem interrupções. Essa abordagem não apenas fortalece a proteção dos dados, mas também aumenta a confiabilidade e resiliência do ambiente de TI, minimizando riscos e assegurando a continuidade dos negócios.

65 Proteção antiDDOS, IDS/IPS e UTM.

▪ A proteção contra DDoS (*Distributed Denial of Service*), junto aos sistemas IDS *(Intrusion Detection System*), IPS (*Intrusion Prevention System*) e UTM (*Unified Threat Management*), é essencial para garantir a segurança da rede e a integridade dos dados organizacionais. A proteção anti-DDoS é projetada para mitigar ataques que visam a sobrecarregar os recursos da rede, assegurando a continuidade das operações. Os sistemas IDS e IPS monitoram e analisam o tráfego em tempo real, identificando atividades suspeitas e respondendo a tentativas de intrusão. O UTM, por sua vez, combina várias funcionalidades de segurança em uma única plataforma, oferecendo uma abordagem integrada para gerenciar e proteger a infraestrutura de TI. Juntas, essas tecnologias formam uma defesa cibernética robusta, proporcionando proteção abrangente contra uma variedade de ameaças e garantindo um ambiente operacional seguro.

66 Canal direto da unidade de segurança com a TI, com atendimento prioritário para questões relacionadas ao ISPS CODE.

▪ Criar um canal direto entre a unidade de segurança com a TI, com atendimento prioritário para questões relacionadas ao ISPS CODE. Exemplo: definir um funcionário que terá dedicação exclusiva ou prioritária no atendimento dos chamados de segurança portuária.

67 Outras ações informadas pelos terminais

▪ Conjunto de boas práticas relacionado aos temas tecnologia, inovação e automação.

▪ Exemplos:

▪ Participação em Hubs de Inovação e Tecnologia (MCI – Melhoria contínua e inovação orgânica da Empresa).

▪ Investimentos permanentes baseados em Plano de Transformação Digital, desenvolvidos pela empresa e aprovados pelos acionistas. Contratação de consultoria, entregando um *roadmap* - PDTI.

▪ Contratação em consultoria de OT (Plano Diretor de Automação e Informação) para os próximos 5 anos.

▪ Auditorias Externas por demanda dos Acionistas.

▪ Criação de TI industrial (segregação de ambientes (OT e TI).

▪ Norma da automação para registro de atualização ou impedimentos – documentação dos Procedimentos de Segurança (Governança de TA OT).

▪ Planejamento de atualizações e ações de OT junto com as paradas programadas / manutenções.

▪ Estrutura corporativa de GRC (Governança, Risco e Conformidade) e ERM (Gerenciamento de Riscos Corporativos).

▪ Sistema de RH automatizado para informar ao gerenciamento de acesso aos SI (cancelamento, revogação e readequação de perfil).

Após a apresentação das melhores práticas voltadas ao fortalecimento da segurança portuária e aduaneira, torna-se oportuno analisar as perspectivas de aprimoramento e os caminhos para a evolução desse sistema. Nesse sentido, o próximo capítulo aborda as oportunidades relacionadas ao aperfeiçoamento das estruturas institucionais, ao uso de novas tecnologias, à integração entre os atores envolvidos e ao desenvolvimento de iniciativas capazes de ampliar a eficiência e a resiliência das operações portuárias.

9- Oportunidades à segurança

Dentro da análise SWOT, as oportunidades são fatores externos e positivos que podem ser aproveitados pela organização ou setor para melhorar seu desempenho, fortalecendo-se no mercado. Em geral, são fatores não controlados pela empresa, ou seja, não dependem exclusivamente da gestão do terminal, mas podem ser aproveitadas estrategicamente em conjunto com órgãos públicos e outras instituições.

No contexto brasileiro da segurança portuária e aduaneira, isso envolve não só as instalações portuárias, mas também a Polícia Federal, a Receita Federal do Brasil (RFB), as Administrações Portuárias e até mesmo instâncias internacionais.

Nesse sentido, a identificação de oportunidades está diretamente relacionada à cooperação interagências, ao aproveitamento de acordos e programas internacionais, à adoção de inovações tecnológicas disponibilizadas por políticas públicas e à convergência com as exigências do comércio exterior e das cadeias logísticas globais.

9.1 Cooperação Interagências

A cooperação interagências é um processo coletivo que envolve diferentes atores — públicos e privados — com funções, mandatos e capacidades distintas, mas que precisam atuar em conjunto para enfrentar problemas complexos. Envolve não apenas somar esforços operacionais, mas também criar um arranjo institucional de governança em rede, capaz de lidar com a complexidade das ameaças em instalações portuárias (Casanova, 2022).

Dentro do contexto da segurança portuária e aduaneira, a cooperação pode ocorrer de diversas formas, como: forças-tarefas (operações conjuntas pontuais), arranjos híbridos de policiamento

(onde os atores possuem competências distintas, mas precisam se alinhar na prática operacional), redes formais coordenadas (a exemplo da própria CONPORTOS, um órgão colegiado deliberativo, de caráter permanente, que reúne diversos atores, como Polícia Federal, Receita Federal, Marinha, e outros já citados nesse trabalho), programa e operações nacionais (Ex: Operação Ágata), além de treinamentos e simulações conjuntas.

A cooperação interagências gera benefícios que vão além da esfera estritamente operacional. A existência de uma rede de segurança integrada aumenta o efeito dissuasório sobre organizações criminosas, ao mesmo tempo em que reduz custos por meio do uso compartilhado de tecnologias e da otimização de esforços, ampliando a capacidade de monitoramento e resposta. Também fortalece a confiança entre Estado e setor privado, estimulando a adesão voluntária a padrões internacionais de segurança, e amplia a competitividade internacional dos terminais portuários brasileiros, tornando-os mais atrativos para armadores e investidores.

Para uma cooperação eficaz e eficiente, sugere-se que algumas medidas sejam implementadas, como a padronização de procedimentos e protocolos operacionais entre as agências, a fim de garantir uma abordagem integrada e consistente na implementação das medidas de segurança nas instalações portuárias, bem como canais de comunicação preestabelecidos que facilitem o fluxo das informações compartilhadas.

Também é recomendável assegurar que as plataformas utilizadas por diferentes agências e empresas sejam compatíveis e possam se integrar facilmente, bem como adotar padrões comuns para garantir que os dados sejam compreendidos e utilizados por todas as partes envolvidas.

Ademais, qualquer espécie de cooperação deve ser coordenada e, para tanto, representantes de cada agência devem ser designados para a comunicação e coordenação da troca de informações. Os envolvidos devem ser constantemente treinados, objetivando destreza na utilização do sistema, garantindo, assim, a correta utilização da plataforma e interpretação das informações recebidas.

Alguns desafios ainda devem ser enfrentados, como diferenças de cultura organizacional, alinhamento de atribuições ou até disputas por recursos, mas com gestores alinhados a essa nova realidade, há grandes possibilidades de progresso nessa área.

Assim, a cooperação interagências é um elemento essencial para promover a segurança integrada e eficaz nas instalações portuárias, garantindo uma resposta coordenada e eficiente diante de possíveis ameaças ou incidentes. No entanto, são vários os desafios para sua implementação.

9.2 Cooperação entre o Público e o Privado

Não há como se falar em segurança, sem envolvermos a colaboração entre entidades públicas (como autoridades portuárias, forças de segurança, agências reguladoras, forças armadas) e entidades privadas (operadores portuários, empresas de transporte, entre outras). Essa sinergia é crucial para garantir a segurança eficaz das instalações portuárias.

Podemos pensar no terminal portuário como uma grande engrenagem, na qual qualquer peça que a emperre pode comprometê-la como um todo. Nos cenários de ameaças à segurança em ambiente portuário, a depender do evento, as informações relevantes podem advir de entes públicos ou privados. Nesse contexto, a cooperação é imprescindível para o sucesso do ambiente de segurança.

Nesse sentido, a Organização Mundial das Aduanas (OMA) preconiza diretrizes para a segurança portuária e aduaneira, consolidadas no Programa Operador Econômico Autorizado (OEA), internalizado no Brasil mediante certificação pela Receita Federal, de empresas que atuam como intervenientes na cadeia logística de comércio internacional, consideradas de baixo risco, configurando uma parceria entre a Aduana e a Empresa para a promoção da segurança contra o tráfico de drogas, por meio da contaminação de cargas lícitas.

A CESPORTOS local, cuja composição já engloba membros da Polícia Federal, Receita Federal, Capitania dos Portos, ANTAQ, unidade de segurança da Autoridade Portuária e Governo do estado (membro convidado), pode e deve promover o engajamento com outros entes públicos e privados, com o objetivo de obter informações e realizar um trabalho de inteligência.

Também deve existir uma troca de informações com os Supervisores de Segurança Portuária, bem como com representantes da prefeitura (controle de trânsito), de concessionária de estradas (controle de tráfego nos acessos ao porto), assim como quaisquer outros entes ou órgãos que possam fornecer ou trocar informações de inteligência as quais sejam úteis para antever e mitigar os problemas de segurança decorrentes do evento.

Destacamos a importância do desenvolvimento de planos de segurança integrados que envolvam tanto as autoridades públicas quanto as empresas privadas, garantindo uma abordagem coordenada e eficiente para proteger as instalações portuárias.

Além disso, o compartilhamento de informações sensíveis e a inteligência entre os setores público e privado contribuem para a identificação de ameaças potenciais, prevenção de incidentes de

segurança e respostas mais eficazes e céleres a emergências.

Frisamos que os exercícios simulados obrigatórios descritos na Resolução 53 da CONPORTOS são ótimas oportunidades para essa integração e cooperação entre funcionários das instalações portuárias, equipes de segurança pública e outros parceiros relevantes para melhorar a prontidão e a capacidade de resposta em caso de incidentes.

Some-se a isso, a possibilidade de integração e compartilhamento de tecnologia e sistemas e câmeras de perímetro da instalação portuária com os órgãos de segurança pública.

A cooperação entre o público e o privado é um pilar fundamental para garantir a segurança eficaz e a proteção das instalações portuárias contra ameaças internas e externas.

9.3 Políticas Públicas e Financiamento

A formulação e implementação de políticas públicas específicas para a segurança portuária e aduaneira constituem importantes oportunidades de fortalecimento.

Um dos principais instrumentos em discussão atualmente é o Plano Nacional de Segurança Pública Portuária (PNSPP), cuja elaboração já foi recomendada pelo Tribunal de Contas da União (TCU). A criação desse plano representa um avanço importante, pois permitirá consolidar diretrizes nacionais, reduzir a fragmentação das ações e alinhar estratégias entre órgãos envolvidos na segurança pública. Para os terminais portuários, trata-se de uma oportunidade de participar ativamente do processo de construção de políticas públicas, garantindo que suas demandas operacionais e de segurança sejam consideradas desde a origem do planejamento

estratégico.

Da mesma forma, as políticas de financiamento também configuram uma oportunidade relevante para o fortalecimento da segurança portuária e aduaneira. Ao disponibilizar recursos específicos para projetos de modernização, essas iniciativas permitem que os terminais ampliem sua capacidade de investimento em infraestrutura crítica, tecnologias de monitoramento e soluções inovadoras de inspeção e análise de risco.

Quando bem aproveitadas, tornam-se instrumentos estratégicos não apenas para reforçar a proteção das instalações contra ilícitos, mas também para promover a inovação tecnológica e a eficiência operacional, alinhando os terminais às melhores práticas internacionais. Nesse sentido, a utilização de financiamentos voltados à segurança possibilita que os terminais se posicionem de forma mais competitiva no comércio global, ao mesmo tempo em que fortalecem a resiliência institucional diante das ameaças contemporâneas.

Após a identificação das oportunidades de aprimoramento e fortalecimento da segurança portuária e aduaneira, torna-se pertinente consolidar as principais reflexões apresentadas ao longo deste Guia. Nesse sentido, o capítulo seguinte apresenta as considerações finais, sintetizando os principais pontos discutidos, reforçando a importância da atuação coordenada entre os diferentes atores e destacando a relevância da adoção contínua de práticas e estratégias voltadas à proteção das operações, das infraestruturas e das cadeias logísticas associadas ao setor portuário e aduaneiro.

10- Conclusão

O **Guia de Melhores Práticas de Segurança Portuária e Aduaneira** consolida-se como uma referência estratégica para o fortalecimento da segurança, da conformidade e da eficiência operacional nas instalações portuárias brasileiras. Ao longo do documento, foram apresentadas práticas fundamentais para a mitigação de riscos, a proteção de ativos e a promoção de um ambiente operacional mais seguro, previsível e resiliente, em consonância com as diretrizes legais e regulatórias vigentes.

A segurança portuária e aduaneira, elementos indissociáveis para a integridade das operações, a proteção de cargas e a segurança dos trabalhadores, foi abordada de maneira abrangente, destacando a importância da integração contínua de tecnologias avançadas, da consolidação de uma cultura organizacional de segurança e da cooperação entre os diversos *stakeholders* do setor.

O uso de tecnologias inteligentes, como sistemas de videomonitoramento (CFTV), drones, dispositivos biométricos e ferramentas de inteligência artificial, tem se mostrado essencial para o monitoramento permanente, a análise de riscos em tempo real e a resposta rápida a incidentes. Essas soluções, ao aliarem precisão operacional e capacidade preditiva, elevam o padrão de proteção das infraestruturas portuárias e reforçam o compromisso com a modernização e a inovação contínua.

Paralelamente, a construção de uma cultura de segurança sólida constitui um dos pilares centrais deste guia. A conscientização permanente e o treinamento sistemático dos colaboradores fortalecem a capacidade das equipes para identificar vulnerabilidades, agir com eficiência diante de emergências e atuar de forma coordenada. Programas de capacitação, exercícios simulados e processos de comunicação interna efetiva garantem o engajamento coletivo e promovem uma responsabilidade compartilhada na manutenção

de padrões elevados de segurança.

Outro vetor essencial é a cooperação institucional entre autoridades públicas, operadores privados e agências de segurança, baseada em intercâmbio de informações e planejamento conjunto. A integração entre os atores, aliada à conformidade com normas internacionais — como o ISPS Code, o SAFE *Framework* da OMA, o Programa OEA e a ISO 31000 —, assegura que as práticas nacionais estejam alinhadas aos padrões globais de segurança e gestão de riscos, reforçando a credibilidade do Brasil nas cadeias logísticas internacionais.

O guia também reconhece a necessidade de responder a múltiplas ameaças contemporâneas, entre as quais terrorismo, roubo de cargas, tráfico de drogas, fraudes aduaneiras, extorsão e ataques cibernéticos. Para cada uma dessas vulnerabilidades, são indicadas medidas preventivas e mitigatórias baseadas nas melhores práticas internacionais, que visam não apenas à proteção das operações, mas também ao fortalecimento da confiança institucional e do ambiente de negócios.

Em síntese, o Guia de Melhores Práticas de Segurança Portuária e Aduaneira representa um instrumento orientador e complementar à legislação vigente, promovendo a adoção contínua de inovações tecnológicas, o aperfeiçoamento das práticas de gestão e o alinhamento entre os diversos entes públicos e privados que integram o setor. Sua implementação requer o comprometimento efetivo de todos os atores, consolidando uma governança colaborativa da segurança, essencial para enfrentar os desafios emergentes, assegurar a continuidade das operações e posicionar o Brasil como um protagonista no comércio internacional seguro e sustentável.

REFERÊNCIAS

ABIN. **Terrorismo**. Brasília, DF, 2020. Disponível em:

https://www.gov.br/abin/pt-br/assuntos/fontes-de-ameacas/terrorismo#:~:text=Posse%20n%C3%A3o%20autorizada%20de%20dados,a%20organiza%C3%A7%C3%B5es%20terroristas%20ou%20extremistas. Acesso em: 14 maio 2025.

ALBUQUERQUE, Carlos Eduardo Pires de; ANDRADE, Felipe Scarpelli de. Análise de Riscos com Ênfase na Segurança Portuária: o processo de avaliação de riscos da CONPORTOS e o ISPS Code**. Revista Brasileira de Ciências Policiais**, Brasília, DF, v. 10, n. 1, p. 99-124, jan./jun. 2019. Disponível em:

https://periodicos.pf.gov.br/index.php/RBCP/article/view/580. Acesso em: 14 maio 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Senado Federal, 1988. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 out. 2025.

BRASIL. **Decreto Nº 9.861, de 25 de junho de 2019**. Dispõe sobre a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis e sobre as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis. Brasília, DF: Presidência da República, 2019. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9861.htm. Acesso em: 14 maio 2025.

BRASIL. **Decreto-Lei Nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em:

https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 14 maio 2025.

BRASIL. **Decreto Nº 10.848, de 26 de outubro de 2021**. Promulga as Emendas ao Anexo à Convenção para a Facilitação do Tráfego Marítimo Internacional adotadas pelo Comitê de Facilitação da Organização Marítima Internacional, entre 1969 e 2005. Brasília, DF: Presidência da República, 2021. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10848.htm. Acesso em: 22 out. 2025.

BRASIL. **Lei Nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei [...]. Brasília, DF: Presidência da República, 1998. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 14 maio 2025.

BRASIL. **Lei nº 13.260, de 16 de março de 2016.** Dispõe sobre o terrorismo, trata de disposições investigatórias e processuais e reforma o Código Penal. Brasília, DF: Presidência da República, 2016. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 22 out. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Resolução Nº 53, de 4 de setembro de 2020**. Dispõe acerca da consolidação

e atualização das Resoluções da Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis [...]. Brasília, DF: Ministério da Justiça e Segurança Pública, 2020. Disponível em:

https://dspace.mj.gov.br/bitstream/1/1599/4/RES_CONPORTOS_2020_53.html. Acesso em: 14 maio 2025.

BRASIL. Polícia Federal. **Conportos.** Brasília, DF,2020. Disponível em:

https://www.gov.br/pf/pt-br/assuntos/seguranca-portuaria/conportos. Acesso em: 14 maio 2025.

BRASIL. Polícia Federal. **PF conclui Operação Mujahidin contra crimes de terrorismo e racismo**. Brasília, DF, 21 mar. 2025. Disponível em:

https://www.gov.br/pf/pt-br/assuntos/noticias/2025/03/pf-conclui-operacao-mujahidin-que-investigou-crimes-de-terrorismo-e-racismo. Acesso em: 22 out. 2025.

BRASIL. Polícia Federal. **Polícia Federal detém entrada de passageiro clandestino pelo Porto de Paranaguá**. Brasília, DF, 29 abr. 2021. Disponível em:

https://www.gov.br/pf/pt-br/assuntos/noticias/2021/04/policia-federal-detem-entrada-de-passageiro-clandestino-pelo-porto-de-paranagua. Acesso em: 25 out. 2025.

BRASIL. Tribunal Regional Federal (4. Região). **Operação Hashtag**: processo tem pedido de vista no TRF4. Porto Alegre, 8 maio 2018. Disponível em:

https://www.trf4.jus.br/trf4/controlador.php?acao=noticia_visualizar&id_noticia=13629. Acesso em: 12 out. 2025.

CASANOVA, Alice Alves. **Networks and ports**: how the concept of security network can foster interagency cooperation in brazilian port security. 2022. Relatório Técnico (Mestrado em Estudos Marítimos) - Escola de Guerra Naval, Rio de Janeiro, 2022. Disponível em:

https://www.marinha.mil.br/ppgem/sites/www.marinha.mil.br.ppgem/files/TCM%20-%20ALICE%20ALVES%20CASANOVA.pdf. Acesso em: 22 out. 2025.

CHECK POINT**. Threat Intelligence Report 2025**. Check Point Software Technologies, 2025. Disponível em:

https://blog.checkpoint.com/. Acesso em: 12 out. 2025.

DP WORLD says hackers stole Australian ports employee data. **Reuters**, Londres, 12 nov. 2023. Disponível em:

https://www.reuters.com/technology/cybersecurity/dp-world-says-hackers-stole-australian-ports-employee-data-2023-11-28/. Acesso em: 12 out. 2025.

ENISA. **ENISA threat landscape 2023**. Attiki: ENISA, Oct. 2023. Disponível em:

https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf?utm_source=chatgpt.com. Acesso em: 22 out. 2025.

ENISA. **ENISA Threat Landscape 2025**. Heraklion: ENISA, Oct. 2025. Disponível em:

https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf. Acesso em: 12 out. 2025.

ESQUADRÃO antibomba é acionado após artefato explosivo ser encontrado em navio no Pará; vídeo. **G1 Pará**, Belém, 19 jun. 2024. Disponível em:

https://g1.globo.com/pa/para/noticia/2024/06/19/esquadrao-antibomba-e-acionado-apos-artefato-explosivo-ser-encontrado-em-navio-no-para-video.ghtml. Acesso em: 22 out. 2025.

FBI. **USS Cole bombing**. [*S. l.*], [2025?]. Disponível em: https://www.fbi.gov/history/famous-cases/uss-cole-bombing. Acesso em: 22 out. 2025.

FORTINET. *Global Threat Landscape Report 2024*. FortiGuard Labs, 2024. Disponível em:

https://www.fortinet.com/reports. Acesso em: 12 out. 2025.

GREEN, Mark E.; MOOLENAAR, John; GIMENEZ, Carlos A. **Handling our cargo**: how the people's Republic of China invests strategically in the U.S. maritime industry. [Washington]: House Committee on Homeland Security Republicans, 2024. Disponível em:

https://homeland.house.gov/wp-content/uploads/2024/09/Joint-Homeland-China-Select-Port-Security-Report.pdf. Acesso em: 22 out. 2025.

IAPH. **IAPH Cybersecurity Guidelines for Ports and Port Facilities**: version 1.0. [*S. l.*], 2021. Disponível em:

https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf. Acesso em: 22 out. 2025.

IAPH. **Port community cyber security**. [*S. l.*, 2020]. Disponível em: https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf. Acesso em: 14 maio 2025.

IMO. **FAL 43/13**: consideration and analysis of reports and information on persons rescued at sea and stowaways. [London], 1 Feb. 2019. Disponível em:

https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Documents/FAL%2043-13.pdf. Acesso em: 10 jun. 2025.

IMO. **Insider Risk in the Maritime Sector**: Recognising and Responding to the Threat. London, [Março de 2024]. Disponível em:

https://indd.adobe.com/view/7c74b606-320b-4dac-939f-a41c291f1b10. Acesso em: 10 jun. 2025.

LYNGAAS, Sean, Japan's largest port hit with ransomware attack. **CNN**, 65 Jul. 2023. Disponível em:

https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack . Acesso em: 12 out. 2025.

PATRIARCA, Gabriel. A âncora da segurança: centralidades e capitais na rede de segurança do Porto de Santos. **Lua Nova**, São Paulo, v. 114, p. 69-104, set./dec. 2021. DOI:

https://doi.org/10.1590/0102-069104/114. Disponível em: https://www.scielo.br/j/ln/a/4Tv3d8pMymBfcQgGkbHmWQj/?lang=pt. Acesso em: 22 out. 2025.

RECEITA FEDERAL. **Portal Aduana e Comércio Exterior, estrutura Aduanas**. Brasília, DF, 2025. Disponível em:

https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior Acesso em: 14 maio 2025.

RECEITA FEDERAL. **Portaria RFB nº 143, de 11 de fevereiro de 2022**. Estabelece normas gerais e procedimentos para o alfandegamento de local ou recinto. Brasília, DF: Receita Federal, 2022. Disponível em:

https://normasinternet2.receita.fazenda.gov.br/#/consulta/externa/123006. Acesso em: 22 out. 2025.

RUSSO FILHO, Antônio. **Comércio internacional**: um modelo para segurança portuária e modernização da aduana brasileira. 2006. Dissertação (Mestrado em Engenharia) – Universidade São Paulo, São Paulo, 2006. Disponível em:

www.teses.usp.br/teses/disponiveis/3/3143/tde-16112006-124645/publico/DISSERTACAO_REVISADA_PDF.pdf. Acesso em: 16 jul. 2024.

UNITED STATES. Customs and Border Protection. **CSI**: Container Security Initiative. 2024. Disponível em:

https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief. Acesso em: 14 maio 2025.

UNITED STATES. Customs and Border Protection. **Customs Trade Partnership Against Terrorism (CTPAT).** 2025. Disponível em: https://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT. Acesso em: 14 maio 2025.

UNODC. Key findings. Viena: UNODC, 2025. Disponível em:

https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf. Acesso em: 22 out. 2025.

WCO. **WCO SAFE Package**: *WCO tools to secure and facilitate global trade*. 2025. Disponível em:

https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/frameworks-of-standards/safe_package.aspx
Acesso em: 14 maio 2025.

ANEXO A - Documentos complementares

1. Organização Marítima Internacional (OMI)

- **Diretrizes de Gestão de Riscos Cibernéticos (MSC-FAL.1/Circ.3):**

  Fornece orientações sobre a gestão de riscos cibernéticos para navios e instalações portuárias. Essas diretrizes cobrem a identificação, proteção, detecção, resposta e recuperação de incidentes cibernéticos.

- **Resolução MSC.428(98) - Gestão de Riscos Cibernéticos na Gestão de Segurança Marítima:**

  Exige que os riscos cibernéticos sejam abordados nas práticas de gestão de segurança dos navios e portos, em conformidade com o Código ISM (Código Internacional de Gestão da Segurança Operacional).

- **Código ISPS (Código Internacional para a Proteção de Navios e Instalações Portuárias):**

  Estabelece requisitos de segurança física e, mais recentemente, cibernética, para instalações portuárias e navios, obrigando os portos a adotar medidas de segurança cibernética em suas operações.

2. International Association of Ports and Harbors (IAPH)

- **Port Community Cybersecurity Guidelines**

  Oferece uma estrutura para que os portos implementem práticas de segurança cibernética, incluindo recomendações para a proteção de dados e resiliência cibernética.

- **Cybersecurity Guidelines for Ports**

  Este documento orienta os portos sobre como gerenciar riscos

cibernéticos, implementar controles de segurança e realizar avaliações regulares de segurança cibernética.

3. NIST (National Institute of Standards and Technology)

- **NIST Cybersecurity Framework:**

  Um *framework* amplamente utilizado para identificar, proteger, detectar, responder e se recuperar de ameaças cibernéticas. Embora seja originário dos EUA, suas práticas são aplicáveis globalmente, incluindo o setor portuário.

- **NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security:**

  Guia para a proteção de sistemas de controle industrial, que são essenciais para as operações portuárias.

4. ISO (International Organization for Standardization)

- **ISO/IEC 27001 - Sistema de Gestão de Segurança da Informação:**

  Norma que define os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação, sendo altamente relevante para o setor portuário.

- **ISO/IEC 27002 - Código de Prática para Controles de Segurança da Informação:**

  Fornece diretrizes para a implementação dos controles de segurança descritos na ISO/IEC 27001.

- **ISO 28000 - Sistema de Gestão de Segurança para a Cadeia de Suprimento:**

  Foca na gestão da segurança ao longo da cadeia de suprimento, incluindo considerações para a segurança cibernética em portos.

5. EU NIS Directive (Diretiva de Segurança de Redes e Sistemas de Informação)

- **Diretiva NIS (2016/1148):**

Estabelece medidas para alcançar um elevado nível comum de segurança das redes e da informação em toda a União Europeia. Aplica-se aos operadores de infraestrutura crítica, incluindo portos.

6. ISACA (Information Systems Audit and Control Association)

- **COBIT (Control Objectives for Information and Related Technologies):**

  Framework de governança e gestão de TI que ajuda as organizações a desenvolverem, implementarem e monitorarem boas práticas de segurança cibernética.

7. BIMCO

- **BIMCO Guidelines on Cyber Security Onboard Ships**

  As diretrizes da BIMCO, uma das maiores associações internacionais de transporte marítimo, também são amplamente adotadas e contêm práticas aplicáveis a terminais portuários.

8. ENISA (Agência da União Europeia para a Segurança Cibernética)

- **Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector:**

  Este relatório fornece boas práticas específicas para o setor marítimo, com foco em portos. Ele abrange a identificação de ameaças, implementação de medidas de segurança e estratégias para mitigar riscos cibernéticos.

- **ENISA Threat Landscape Reports:**

  Relatórios anuais que detalham as ameaças cibernéticas mais recentes e emergentes em vários setores, incluindo o marítimo. Eles ajudam a entender o panorama de ameaças e a adaptar as medidas de segurança de acordo.

- **Guidelines for Cybersecurity in the Maritime Sector:**

  Diretrizes que abordam os desafios de segurança cibernética

enfrentados pelo setor marítimo, com recomendações para melhorar a resiliência cibernética de navios e portos.

- **NIS Directive Implementation Guidance:**
  A ENISA também fornece orientações sobre a implementação da Diretiva NIS, que é crucial para operadores de infraestrutura crítica, incluindo portos.

9. IET (Institution of Engineering and Technology) do Reino Unido

- **Code of Practice: Cyber Security for Ports and Port Systems:**
  Este código de prática, desenvolvido pelo IET, é uma referência essencial para a segurança cibernética em ambientes portuários. Ele fornece uma estrutura abrangente para a implementação de controles de segurança cibernética, abordando aspectos como gerenciamento de riscos, proteção de sistemas críticos e resposta a incidentes.

Realizado o Depósito legal na Biblioteca Nacional conforme a Lei nº 10.994, de 14 de dezembro de 2004.

TÍTULO	Guia de Melhores Práticas de Segurança Portuária e Aduaneira
AUTOR	Sérgio Cutrim
CAPA	Dyego Santos Nolasco
PROJETO GRÁFICO	Carlos Eduardo Sales
IMAGENS	freepik.com
PÁGINAS	143
TIPOGRAFIA	Segoe UI Variable regular | CORPO Segoe UI Variable light | TÍTULOS

ABEPH ABRATEC ABTL ABTRA ABTP ATP FENOP

ISBN 978-655363532-6

EDUFMA