Escola de Guerra Naval – Fundação Ezute

ANÁLISE DOS MODELOS DE GOVERNANÇA DOS PORTOS EM SEGURANÇA CIBERNÉTICA

Relatório de Pesquisa

Grupo de Pesquisa EGN-EZUTE

2022-2023

ESCOLA DE GUERRA NAVAL

FUNDAÇÃO EZUTE

ACORDO DE COOPERAÇÃO TÉCNICA EGN-EZUTE

PLANO DE TRABALHO PARA O PERÍODO 2022 – 2023

PROJETO DE PESQUISA EGN-EZUTE

ANÁLISE DOS MODELOS DE GOVERNANÇA DOS PORTOS EM SEGURANÇA CIBERNÉTICA.

RIO DE JANEIRO

2023

APRESENTAÇÃO

Este relatório técnico aborda o tema “Análise dos Modelos de Governança dos Portos em Segurança Cibernética”, atinente ao projeto de pesquisa aplicada desenvolvido no âmbito da parceria entre a Fundação Ezute e a Escola de Guerra Naval (EGN), por intermédio da Superintendência de Pesquisa e Pós-Graduação (SPP) e do Programa de Pós-Graduação em Estudos Marítimos (PPGEM). A iniciativa foi apoiada pelo Centro de Estudos Político-Estratégicos da Marinha (CEPE-MB).

O trabalho se desenvolveu em conformidade com o plano de trabalho estabelecido para o biênio 2022-2023. O grupo de pesquisa foi composto por professores, profissionais e mestrandos do PPGEM-EGN e pesquisadores da EZUTE. O trabalho se desenvolveu por meio de pesquisa bibliográfica e documental, complementada por reuniões de trabalho, seminários e outras atividades, para as quais contribuíram colaboradores externos convidados.

Registra-se, assim, o agradecimento do grupo de pesquisa à EGN e à Ezute pelo apoio e pelo estímulo concedidos, bem como aos colaboradores convidados, pelas contribuições que proporcionaram.

INSTITUIÇÕES PARTICIPANTES

Escola de Guerra Naval – EGN

Avenida Pasteur, n. 480 – Urca
CEP: 22290-240-Rio de Janeiro- RJ
Tel.: (21) 2546-9325 / 9326

Fundação Ezute

Rua do Rocio, n. 313, 11º andar-Vila Olímpia
CEP: 04552-904-São Paulo- SP
Tel.: (11) 3040-7300 / 7400

GRUPO DE PESQUISA – EQUIPE TÉCNICA

Coordenadores:

- Dr. Cleber Almeida de Oliveira (Fundação Ezute);
- Dr. José Roberto Brito de Souza (EGN);
- Prof. Dr. Nival Nunes de Almeida (EGN);

Pesquisadores Colaboradores:

- M. Sc. Claudia de Andrade Tocantins (Fundação Ezute);
- Dr. Leandro da Silva Teixeira (Fundação Ezute);

Mestrandos e Pesquisadores EGN:

- Fernanda Gomes de Carvalho (PPGEM-EGN);
- Vivian de Mattos Marciano (PPGEM-EGN).

RESUMO

O presente relatório tem como propósito analisar portos brasileiros quanto à segurança cibernética de seus dados de tráfego e sugerir melhorias a partir da comparação com o modelo de governança de dados dos portos europeus. A pesquisa realizada é primordialmente qualitativa e exploratória. Para atingir tal propósito, este trabalho está organizado em cinco seções, além de uma introdução. Na segunda seção, o contexto portuário é descrito. Na terceira seção os conceitos de governança corporativa e governança portuária são explicados. A quarta seção, discute o conceito de dados marítimos compartilhados e o modelo de gerenciamento desses dados nos principais portos da região Sudeste do Brasil. Em seguida, a quinta seção descreve as proposições europeias sobre segurança cibernética dos dados de tráfego marítimo, o arcabouço documental brasileiro sobre o assunto e as sugestões de melhoria para os portos brasileiros. Por fim, no sexto capítulo as considerações finais são apresentadas.

Palavras chaves: Governança Portuária; Segurança Cibernética e Complexo Portuário

ABSTRACT

The purpose of this report is to analyze Brazilian ports regarding the cybernetic security of their traffic data and suggest improvements based on the comparison with the data governance model of European ports. The research conducted is primarily qualitative and exploratory. To achieve this purpose, this paper is organized in six sections, besides an introduction. In the second section, the port context is described. In the third section, the concepts of corporate governance and port governance are explained. The fourth section discusses the concept of shared maritime data and the management model of this data in the main ports of the Southeast region of Brazil. Then, the fifth section describes the European propositions on cybersecurity of maritime traffic data, the Brazilian documentary framework on the subject and suggestions for improvement for Brazilian Ports. Finally, the final considerations are presented in the sixth section.

Keywords: Port Governance; Cybersecurity and Port Complex.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ANEXOS

SUMÁRIO

1 INTRODUÇÃO

Em 2018 a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) constatou que cerca de 80% do comércio mundial, em volume, é feito pelos mares[1]. Portanto, os portos exercem um papel relevante, viabilizando a infraestrutura operacional, gestão dos dados e informações do comércio marítimo para o envio e para o recebimento de mercadorias, bem como na interação com as diversas partes interessadas na movimentação portuária.

No presente relatório, objetiva-se pensar os portos brasileiros e suas possibilidades de melhoria quanto à segurança cibernética de seus dados de tráfego a partir da análise dos modelos utilizados pelos portos europeus. Dessa forma, serão analisados os fluxos de informações dos serviços de tráfego de embarcações (*Vessel Traffic Service* -VTS) e dos sistemas de informações e gerenciamento do tráfego de embarcações (*Vessel Traffic Management Information System* - VTMIS) nos principais portos da região sudeste e as medidas de segurança cibernética a eles aplicada. Para tal, é preciso entender o contexto portuário e quais são os entes que atuam dentro deste ambiente.

[1] Disponível em: https://unctad.org/publication/review-maritime-transport-2021. Acesso em: 03 de março de 2022.

2 CONTEXTO PORTUÁRIO

A União Europeia, bloco que possui alguns dos portos mais movimentados do mundo, define porto, por meio da diretiva 2005/65/EC, como sendo "qualquer área especificada de terra e água, com fronteiras definidas pelo Estado membro no qual o porto está localizado, contendo serviços e equipamentos designados para facilitar o transporte marítimo comercial." (ENISA, 2019)[2]. Por essa definição é possível perceber que o Estado tem grande poder de gestão sobre os portos, justamente por conseguir delimitar sua área e, consequentemente, sua localização.

As dinâmicas público-privadas que predominam na gestão dos portos da Europa são as do *Landlord port*[2] e do *Tool port*[3], segundo a classificação feita pelo Banco Mundial. Com exceção dos portos britânicos, em que há a predominância da gestão dos portos pela iniciativa privada (BRITTO *et al*, 2015).

É válido ressaltar que a legislação brasileira não define o que seria um simples "porto". Segundo o dicionário Michaelis, a definição de porto é: **1** ANT Acesso por terra (...); **5** Área marítima, fluvial ou lacustre, com profundidade considerável e instalação apropriadas, que viabilizam o atracamento de embarcações, além da comunicação com o pessoal em terra.

A lei brasileira nº 12.815/2013, define o "porto organizado" como:

> (...) bem público construído e aparelhado para atender a necessidades de navegação, de movimentação de passageiros ou de movimentação e armazenagem de mercadorias, e cujo tráfego e operações portuárias estejam sob jurisdição de autoridade portuária.

A mesma lei considera que a área do porto organizado deve ser delimitada por ato do Poder Executivo que compreende as instalações portuárias e a infraestrutura de proteção e de acesso ao porto organizado.

A instalação portuária é definida como qualquer instalação localizada dentro ou fora da área do porto organizado e utilizada em movimentação de passageiros e em movimentação ou armazenagem de mercadorias, destinadas ou provenientes de transporte aquaviário. Sendo assim, conforme ilustrado na Figura 1, pode-se identificar dois tipos de Instalações Portuárias: as públicas e as privadas.

---

[2] Modelo em que a gestão, supervisão e regulamentação do porto e de suas atividades são feitas pelo Estado, enquanto a prestação de serviços e atividades mais operacionais são realizadas por agentes privados (BRITTO *et al*, 2015).

[3] Modelo em que a iniciativa privada atua apenas em atividades de operação dentro dos terminais, como por exemplo a carga e descarga de navios, enquanto o Estado se torna responsável pelas demais atividades (BRITTO *et al*, 2015).

Figura 1- Fluxograma dos Tipos de Instalações Portuárias
Fonte: Elaboração Própria.

Os terminais de uso privado, as estações de transbordo de carga e as instalações públicas de pequeno porte são instalações portuárias que ficam fora da área do porto organizado e exploradas mediante autorização. Há também aquelas voltadas para o turismo, em que o uso pode ser feito via arrendamento ou autorização do governo federal, e cuja finalidade é embarcar e desembarcar pessoas e insumos ligados à atividade turística.

A regulamentação do sistema portuário brasileiro sofreu várias mudanças ao longo do tempo. De 1934 a meados da década de 90, o modelo de gestão portuária do Brasil era integralmente estatal. Em 1993, com a lei nº 8.630/93, o governo brasileiro abriu o setor para o capital privado (BRITTO *et al*, 2015). Já em 2013, a lei nº 12.815/2013 dispôs sobre a exploração direta e indireta pela União de Portos e Instalações Portuárias e sobre as atividades desempenhadas pelos operadores portuários. De acordo com FARRANHA *et al* (2015), o objetivo foi aumentar a competitividade dos portos brasileiros a partir de uma maior participação da iniciativa privada e com a modernização dos processos.

No setor portuário moderno, a prestação eficiente dos serviços de movimentação de carga está condicionada ao uso de equipamentos especializados por tipo de carga, justificando a tendência atual de segmentação e especialização, dentro de um porto, das atividades de movimentação de carga (ESTACHE E RUS, 2000).

A resolução normativa nº7 (2016) da Agência Nacional de Transportes Aquaviários (ANTAQ)[4] regulou a exploração de áreas e instalações portuárias sob gestão da Administração do Porto, no âmbito dos Portos Organizados, considerando a seguinte definição do artigo 2°: "para efeitos desta Norma, considera-se: I – administração do porto organizado: a autoridade portuária exercida diretamente pela União, por suas controladas, pela delegatária ou pela concessionária do porto organizado".

Após compreender alguns conceitos portuários e algumas dinâmicas implicadas, tanto pelo governo brasileiro quanto pela União Europeia, serão expostos a seguir os principais

[4] Disponível em: https://juris.antaq.gov.br/index.php/2016/06/02/resolucao-normativa-no-07-2016/. Acesso em: 15 de junho de 2022

stakeholders públicos e privados que compõem o complexo portuário, apresentando qual é o seu papel dentro dos portos.

Como a Lei dos Portos não define os papéis a serem exercidos por todos os stakeholders de interesse dentro dos portos, este estudo buscou definições nas resoluções de agências reguladoras e de Autoridades Portuárias para complementar esse déficit conceitual.

O esforço de compreender os entes envolvidos no complexo portuário deriva da necessidade de entender quais são as partes envolvidas na gestão dos dados e das informações portuárias no Brasil.

2.1 Autoridade Marítima (AM)

As atribuições da Autoridade Marítima (AM), exercida pelo Comandante da Marinha, são de promover a implementação e a execução da lei nº 9537/1997 (BRASIL, 1997) com o propósito de assegurar a salvaguarda da vida humana e a segurança da navegação, no mar aberto e hidrovias interiores, e a prevenção da poluição ambiental por parte de embarcações.

Dessa forma, a AM deve estabelecer normas que assegurem o referido propósito, tais como a NORMAM 26, norma da autoridade marítima para o serviço de tráfego de embarcações, que regula o funcionamento dos VTS no país.

2.2 Autoridade Portuária (AP)

A lei 12815/2013 (BRASIL, 2013) define a Autoridade Portuária (AP) como a administração do Porto Organizado e estabelece as suas atribuições, dentre elas autorizar a entrada e saída, inclusive atracação e desatracação, o fundeio e o tráfego de embarcações na área do porto, ouvidas as demais autoridades do porto.

Conforme a NORMAM 26, cabe às Autoridades Portuárias (AP) e aos Operadores de Terminais de Uso Privado (categorizados como provedores de VTS), a implantação, gestão, operação e coordenação das atividades do VTS.

2.3 Órgãos Governamentais

2.3.1 Receita Federal

A Receita Federal é a parte integrante do Ministério da Fazenda que tem como missão administrar "o sistema tributário e aduaneiro, contribuindo para o bem-estar econômico e social do país (BRASIL, 2013). Dentro do arcabouço portuário, a Receita é:

> [...] unidade responsável por fiscalizar a entrada, permanência, movimentação e saída de pessoas, veículos e cargas das instalações portuárias alfandegadas. Responde pela vigilância aduaneira e repressão ao contrabando e descaminho, bem como pela arrecadação dos tributos incidentes sobre o comércio exterior e pelo despacho aduaneiro na importação e exportação (SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS.).

A seção II da Lei dos Portos estabelece as competências da administração aduaneira nos portos organizados e nas instalações portuárias alfandegadas.

2.3.2 Capitania dos Portos

A Capitania dos Portos[5], vinculada à Autoridade Marítima por meio da Diretoria de Portos e Costas, trabalha com objetivo de:

> [...] contribuir para a orientação, coordenação e controle das atividades da Marinha Mercante. Fiscaliza os serviços de praticagem, realiza inspeções navais, conduz inquéritos administrativos de acidentes de navegação, auxilia o serviço de salvamento marítimo, mantém a sinalização náutica, entre outros (AUTORIDADE PORTUÁRIA DE SANTOS, S.A).

2.3.3 Núcleo Especial de Polícia Marítima (NEPOM)

O Núcleo Especial de Polícia Marítima (NEPOM), vinculado ao Departamento da Polícia Federal (DPF), objetivam, principalmente, a prevenção e a repressão aos ilícitos praticados a bordo, contra ou em relação a embarcações na costa brasileira e, a fiscalização do fluxo migratório no Brasil (entrada e saída de pessoas), sem prejuízo da prevenção e repressão aos demais ilícitos de competência do DPF, inclusive estendendo-se além do limite territorial,

[5] Vale frisar que a Capitania dos Portos representa um conglomerado de 32 organizações dispostas em 9 Distritos Navais. Dessa forma, cada porto fará parte da capitania dos portos do seu estado. Para mais informações, acesse: https://www.marinha.mil.br/dpc/node/3503

quando se fizer necessário e observadas as normas específicas da Marinha do Brasil (BRASIL, 1999, p.1).

2.3.4 Sistema de Vigilância Agropecuária Internacional (VIGIAGRO)

O Sistema de Vigilância Agropecuária Internacional (VIGIAGRO), vinculado ao Ministério da Agricultura, Pecuária e Abastecimento, objetiva supervisionar as cargas de origem animal ou vegetal movimentadas no porto, atestando sua qualidade e origem (SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS).

2.4 Agências Reguladoras e Autarquias

Segundo Azevedo (S.A), com base na Lei n. 4.595/64, as agências reguladoras foram "criadas para o controle e para a fiscalização dos serviços públicos concedidos — atividades típicas do Estado — mas atuando de forma descentralizada, com autonomia técnica, administrativa e financeira". Considerando tal conceito, a autoridade portuária de Santos define que há a atuação de três agências reguladoras em seu perímetro, sendo elas: a Agência Nacional de Transportes Aquaviários (ANTAQ); a Agência Nacional de Vigilância Sanitária (ANVISA) e a autoridade ambiental que abarca Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA) e a Companhia Ambiental do Estado.

2.4.1 ANTAQ

A ANTAQ dentro da estrutura portuária é uma: "autarquia vinculada ao Ministério da Infraestrutura. Regula, supervisiona e fiscaliza as atividades de prestação de serviços de transporte aquaviário e de exploração da infraestrutura portuária e aquaviária.

Segundo a Lei dos Portos, todas as infraestruturas portuárias devem prestar "informações de interesse do poder concedente, da ANTAQ e das demais autoridades que atuam no setor portuário, inclusive as de interesse específico da Defesa Nacional, para efeitos de mobilização" (BRASIL, 2013, p.3). Sendo assim, a ANTAQ deve ter inclusive acesso aos portos, sendo ela responsável pela fiscalização e regulação portuária. Segundo o artigo VII da Lei dos Portos: "A ANTAQ poderá disciplinar a utilização em caráter excepcional, por qualquer interessado, de instalações portuárias arrendadas ou exploradas pela concessionária, assegurada a remuneração adequada ao titular do contrato" (BRASIL, 2013, p.5). Compreende-se assim,

que a ANTAQ além de ser uma agência fiscalizadora e reguladora, é responsável também pela articulação com "órgãos e entidades da administração, para resolução das interfaces do transporte aquaviário com as outras modalidades de transporte, com a finalidade de promover a movimentação intermodal mais econômica e segura de pessoas e bens" (BRASIL, 2013, p.9).

2.4.2 ANVISA

A ANVISA é vinculada ao Ministério da Saúde e visa a responder pelo controle sanitário em meios de transportes, viajantes, infraestrutura, produtos importados e exportados, serviços e bens produzidos, bem como pela vigilância epidemiológica e controle de vetores. Emite o Certificado de Livre Prática, que libera a embarcação para operar no porto (SANTOS, S.A).

2.4.3 Autoridades Ambientais

As autoridades ambientais, sendo o IBAMA a nível federal e a Companhia Ambiental do Estado a nível estadual, são responsáveis pelo controle, fiscalização, monitoramento e licenciamento de atividades geradoras de poluição com a preocupação fundamental de preservar e recuperar a qualidade das águas, do ar e do solo.

Na perspectiva ambiental, a lei dos portos insere outro *player* implantado pela Secretaria de Portos da Presidência e pelo Ministério dos Transporte, o Programa Nacional de Dragagem Portuária e Hidroviária II que também é responsável pelo monitoramento ambiental junto com outras funções como:

> [Realizar] I - as obras e serviços de engenharia de dragagem para manutenção ou ampliação de áreas portuárias e de hidrovias, inclusive canais de navegação, bacias de evolução e de fundeio, e berços de atracação, compreendendo a remoção do material submerso e a escavação ou derrocamento do leito; II - o serviço de sinalização e balizamento, incluindo a aquisição, instalação, reposição, manutenção e modernização de sinais náuticos e equipamentos necessários às hidrovias e ao acesso aos portos e terminais portuários; III - o monitoramento ambiental; e IV - o gerenciamento da execução dos serviços e obras (BRASIL, 2013, p. 15).

2.5 Arrendatários, Autorizatários e Operadores

Os arrendatários, autorizatários e os operadores atuam na exploração da operação portuária, e que consequentemente necessitam compartilhar as informações do complexo portuário para desempenhar suas funções.

Os arrendatários são empresas que:

> [...] detém o direito de exploração de área afetada pela operação portuária dentro dos limites do Porto Organizado. Os arrendatários são os responsáveis pelos Terminais Portuários onde se realizam os embarques, descargas e armazenamento das mercadorias. O Porto possui terminais especializados na operação de carga geral, conteinerizada, veículos, granéis (sólidos e líquidos) e passageiros. Os arrendamentos de terminais dentro do Porto Organizado são feitos por meio de contratos, precedidos de licitação realizada pela ANTAQ (SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS.).

Como exemplo, pode-se citar duas empresas arrendatários do agronegócio, a ADM do Brasil e a Bunge, dentro do Porto de Santos, que atuam conforme a citação anteposta, possuindo terminais próprios dentro do complexo portuário de Santos (SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS).

Os autorizatários, assim como os arrendatários, são empresas que possuem o direito de exploração de área afeta à operação portuária. Entretanto, os arrendatários têm tal autorização para atuar dentro dos limites do Porto Organizado[6], já os autorizatários não, eles só podem atuar fora dos limites do Porto Organizado.

Segundo o Ministério da Fazenda e a Lei dos Portos, o operador portuário é a pessoa jurídica pré-qualificada para exercer as atividades de movimentação de passageiros ou movimentação e armazenagem de mercadorias, destinadas ou provenientes de transporte aquaviário, dentro da área do porto organizado" (BRASIL, S.A, p.1)[7].

A operação portuária em instalações localizadas fora da área do porto organizado será disciplinada pelo titular da respectiva autorização, observadas as normas estabelecidas pelas autoridades marítima, aduaneira, sanitária, de saúde e de polícia marítima.

---

[6] Segundo o Ministério de Infraestrutura, "Os incisos I e II do art. 2º da Lei nº 12.815/2013 estabelecem os conceitos de "porto organizado" e "área do porto organizado". "Porto organizado" é o conjunto de bens públicos necessários à consecução das atividades portuárias dentro de um espaço geográfico, chamado de "área do porto organizado". A "área do porto organizado é uma parte dos bens públicos que compõem o "porto organizado"

[7] (BRASIL, S.A, p.1). Acesso em: https://www.gov.br/infraestrutura/pt-br/assuntos/transporte-aquaviario/poligonais#:~:text=%22Porto%20organizado%22%20%C3%A9%20o%20conjunto,comp%C3%B5em%20o%20%22porto%20organizado%E2%80%9D.

2.6 Armadores, Agentes e Despachantes

Os armadores são os responsáveis por proporcionar o transporte marítimo de cargas locais ou internacionais, tendo em vista que eles são os donos das embarcações.

Os agentes marítimos são os representantes de armadores nos portos e respondem pelo suprimento das necessidades materiais dos navios e pela intermediação comercial. É o elo entre os donos dos navios e os intervenientes públicos e privados do processo de exportação/importação

Os despachantes aduaneiros representam os importadores, exportadores, transportadores e armazéns alfandegados perante órgãos governamentais nos procedimentos aduaneiros, fiscais, tributários, logísticos e comerciais para liberação aduaneira (AUTORIDADE PORTUÁRIA DE SANTOS, S.A, p.1).

2.7 Fornecedores de Bens e Serviços Portuários

Estes *stakeholders* são os responsáveis por fornecer materiais e serviços para a autoridade portuária, a fim de que o porto possa desempenhar suas funções. A Autoridade Portuária pode segmentar tais *players* em seis tipos de empresas, sendo elas:

i) amarração: empresas que realizam os serviços de amarração, desamarração e puxada de navios nos berços;

ii) bunker: empresas que fornecem combustíveis;

iii) rebocadores: empresas que operam no apoio a manobras de navios, atuando nos serviços de atracação e desatracação;

iv) Consumo: empresas que fornecem materiais de consumo de bordo como alimentos, bebidas, peças e outros equipamentos para o uso das embarcações mercantes;

v) Órgão Gestor de Mão de Obra (OGMO): empresa responsável pelo fornecimento de mão de obra do trabalhador portuário avulso (TPA) para realização das operações portuárias; e

vi) Praticagem: empresa que vai desde a assessoria, quanto a realização de entrada e saída de embarcações do porto, coordenando o tráfego marítimo e gerenciando os riscos navais em águas restritas (SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS., p.1).

No quadro abaixo são especificados quais stakeholders são definidos por quais entes institucionais, para que assim o leitor tenha uma visão mais clara dessa discussão. Vale ressaltar que a Tabela 1 visa a expor a incompletude da Lei dos Portos e a falta de instrumentos jurídicos federais que conceituem de forma robusta os stakeholders portuários. Dessa forma, não serão apresentados órgãos estaduais ou municipais que façam parte desse circuito, como é o caso das Companhias Ambientais dos estados.

Tabela 1: Localização da Conceituação dos Stakeholders Portuários de Nível Federal

Localização da conceituação dos stakeholders portuários de nível federal			
Stakeholder	**Lei dos Portos**	**ANTAQ**	**Autoridade Portuária do Porto de Santos**
ANTAQ	Presente em todo documento como principal órgão fiscalizador das atividades portuárias	-	Classificada como agência reguladora
ANVISA	Não menciona de forma direta	Não menciona de forma direta	Classificada como agência reguladora
IBAMA	Não menciona de forma direta	Não menciona de forma direta	Classificada como autoridade ambiental
Receita Federal	Não menciona de forma direta	Não menciona de forma direta	Classificada como órgão governamental
Capitania dos Portos (Marinha do Brasil)	A Marinha do Brasil é citada como autorizada a realizar operações de emergência nos portos a qualquer momento	Não menciona de forma direta	Classificada como órgão governamental
Polícia Federal	Não menciona de forma direta	Não menciona de forma direta	Classificada como órgão governamental
Arrendatários	Não menciona de forma direta	Definidos no artigo 2º, parágrafo 7º da resolução normativa nº7/2016	Empresas com direito de exploração de determinadas áreas dentro do porto organizado, responsáveis pelos terminais portuários.
Autorizatários	Apenas citado no artigo 8º, parágrafo 5º, §2	Não menciona de forma direta	Empresas com direito de exploração de determinadas áreas fora do porto organizado
Operadores Portuários	Definidos no artigo 2º, parágrafo 8º da Lei dos Portos	Definidos no artigo 2º, parágrafo 15º da resolução normativa nº7/2016	Conceituados de acordo com a Lei dos Portos

Localização da conceituação dos stakeholders portuários de nível federal			
Stakeholder	**Lei dos Portos**	**ANTAQ**	**Autoridade Portuária do Porto de Santos**
Agentes Marítimos	Não menciona de forma direta	Não menciona de forma direta	"Representantes dos Armadores nos portos" (AUTORIDADE PORTUÁRIA DE SANTOS, S.A, p.1)
Armadores	Não menciona de forma direta	Não menciona de forma direta	Definidos como sendo os donos das embarcações
Despachantes Aduaneiros	Não menciona de forma direta	Não menciona de forma direta	Definidos como representantes dos importadores, exportadores e transportadores ante os órgãos governamentais
Fornecedores de bens e serviços portuários	Não menciona de forma direta	Não menciona de forma direta	São as empresas de armação, bunkers, rebocadores, fornecedoras de alimentos para consumo de bordo, Órgão Gestor de Mão de Obra (Ogmo) e a praticagem
Autoridade Portuária	Apenas mencionada no artigo 17º, §1, sem uma maior definição conceitual	Definida no artigo 2º, parágrafo 1º da resolução normativa nº7/2016	Não menciona de forma direta
Usuários	Não menciona de forma direta	Definido no artigo 2º, parágrafo 28º da resolução normativa nº7/2016	Não menciona de forma direta
Empresa de Navegação	Não menciona de forma direta	Definido no artigo 2º, parágrafo 12º da resolução normativa nº7/2016	Não menciona de forma direta

Fonte: Elaboração Própria.

Após compreender a definição de porto e quais são os *stakeholders* que atuam no complexo portuário, precisa-se definir o que é governança e os tipos que são observados no complexo portuário no novo cenário mundial de fluxos informacionais portuários. Dessa forma, a próxima seção se esforçará em compreender tais conceitos.

3 GOVERNANÇA CORPORATIVA E GOVERNANÇA PORTUÁRIA

Devido a abertura de novos mercados após o fim da Guerra Fria nos anos 1990, ocorreu internacionalmente uma dinamização e interconexão das economias globais e consequentemente da movimentação do fluxo de cargas, criando-se cadeias produtivas mais complexas. Este novo cenário mundial desafiador demandou e tem demandado por parte dos portos uma reestruturação devido a quantidade de informações e de dados que devem ser gerenciados, a fim de realizar uma boa gestão dos processos operacionais portuários. Considerando o cenário desafiador anteposto, os portos precisam se adequar ao novo fluxo de informações, prezando sempre pela otimização dos recursos, pelo menor tempo de estadia dos navios nos portos e maior produtividade na movimentação de carga. Dessa forma, segundo a ANTAQ:

> Com o aumento dos fluxos portuários é necessário um processo de modernização da gestão portuária baseada em um sistema de informações logísticas que auxiliará um planejamento operacional integrado entre os complexos portuários com foco nos indicadores de desempenho econômico (ANTAQ, 2018, p.2).

Dessa forma, nesta seção dois conceitos serão explorados: i) o de governança corporativa, pois os portos atuam como empresas e; ii) governança portuária, pois apesar de serem empresas, os portos possuem suas respectivas particularidades, como será apresentado.

Gonçalves (2005) apresenta que a expressão em inglês "*governance*" aparece em discussões atuais que têm a finalidade de conhecer as condições que fazem ou trazem a eficiência do Estado em seu caráter mais amplo e particular, indo dos aspectos da alta política, economia e suas dimensões sociais para que o Estado possa criar políticas públicas mais assertivas de acordo com sua realidade. Assim, o Estado consegue se guiar "pelos resultados das políticas governamentais, [...] também a forma pela qual o governo exerce o seu poder" (GONÇALVES, 2005, p.1). Assim, o autor define:

> [A] definição geral de governança é o exercício da autoridade, controle, administração, poder de governo. Precisando melhor, é a maneira pela qual o poder é exercido na administração dos recursos sociais e econômicos de um país visando ao desenvolvimento, implicando ainda na capacidade dos governos de planejar, formular e implementar políticas e cumprir funções (GONÇALVES, 2005, p.1-2).

Entende-se assim que ter uma boa governança é essencial para a aquisição de um desenvolvimento sustentável no longo prazo, incorporando ao crescimento econômico, outras variáveis sociais como direitos humanos e equidade social (GONÇALVES, 2005, p.2). Além disso, Gonçalves (2005, p.2) ressalta a importância da criação de metas institucionais que auxiliem no direcionamento e nas tomadas de decisão entre os agentes da burocracia estatal, mas também dos agentes privados envolvidos na administração.

3.1 Governança Corporativa

Trabalhar com o conceito de governança corporativa em um aspecto de estudos portuários passa pela premissa de compreender que os portos são empresas. De acordo com o código de processo civil de 2002, no seu artigo 966, "Considera-se empresário [ou empresa] quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços". Dessa forma, haja vista ao conceito de porto que foi apresentado na seção anterior, é possível afirmar que portos são empresas, o que faz com que trabalhar o conceito de governança corporativa não seja só pertinente como também necessário. Esses portos podem ser empresas públicas, privadas ou sob licitação (TOMAZETTE, 2018, p.2).

Segundo Vieira (S.A, p. 1), o conceito de governança corporativa é um "sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas a crescer, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização, controle e demais partes interessadas".

Já o Instituto Brasileiro de Governança Corporativa (IBGC) apresenta a seguinte conceituação:

> [...] as práticas e os relacionamentos entre os Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal, com a finalidade de otimizar o desempenho da empresa e facilitar o acesso ao capital, e ela surge, a partir da teoria econômica tradicional, para superar o chamado "conflito de agência", presente com a separação entre a propriedade e a gestão empresarial (GONÇALVES, 2005, p.2).

Apesar de serem fontes distintas, ambos os conceitos são similares ao entenderem que a governança corporativa visa a orientar todos os stakeholders da empresa, sejam internos, externos, independentemente do nível hierárquico, sobre como se deve agir, monitorar e se

relacionar, gerindo conflitos, a fim de focar no crescimento, no desenvolvimento da corporação, dando o rumo necessário aos negócios para que todas as partes estejam envolvidas e alinhadas com os respectivos propósitos da empresa.

3.2 Governança Portuária

Considerando que dentro do espectro empresarial, o foco deste relatório são os portos, será necessário apresentar o conceito de governança portuária. De acordo com Vieira e Fialho (2020, p. 2), a governança portuária é um

> [...] mecanismo utilizado para coordenar as relações existentes entre os atores nos processos operacionais da cadeia logística portuária. Em busca do melhoramento contínuo, aumento a eficiência e a eficácia dos fluxos logísticos e consequentemente a competitividade do porto.

Segundo Sousa et. al (2019), a governança corporativa está relacionada a autoridade portuária, a gestão de todo o complexo portuário como um todo, e a governança portuária está: "mais relacionada à governança da aglomeração empresarial, que abrange desde o porto até os diversos atores envolvidos na operação portuária" (SOUSA et. al, 2019.p.765). Sendo assim, em termos de governança portuária, leva-se em consideração "o conjunto de atores que realizam atividades direta ou indiretamente relacionadas aos portos" (SOUSA et. al, 2019.p.765).

A governança portuária visa a aumentar, a promover e a organizar toda a performance da cadeia logístico-portuária, maximizando a eficiência do sistema portuário. O olhar debruçado na eficiência portuária é tão relevante que acaba sendo um elemento no processo de tomada de decisão em diversas escolhas que impactam a operação portuária como a escolha dos armadores, como dos exportadores, importadores ou agentes de cargas (SOUSA et. al, 2019.p.766).

Dentro do conceito de governança portuária, é necessário que se construa um modelo alicerçado nos resultados, sejam quantitativos ou qualitativos. Por meio dos resultados, os desafios e oportunidades devem ser identificados, a fim de obter um aumento de eficiência na operação portuária, estabelecendo-se assim ações de governança que façam a coordenação "dos atores e a melhoria das atividades da cadeia logístico-portuária, condicionados à estrutura da governança existente" (SOUSA et. al, 2019.p.766).

Tendo em vista que o objetivo principal deste trabalho é analisar o uso dos VTS e VTMIS nos principais portos da região sudeste e as medidas de segurança cibernética a eles aplicada, o capítulo que se seguirá irá debater quais são os portos que já utilizam tal tecnologia e como é feita a gestão dos dados obtidos, contribuindo para a governança portuária.

4 GERENCIAMENTO DE DADOS DE TRÁFEGO MARÍTIMO

Uma vez tendo compreendido a breve explicação sobre o que é um porto e como é feita sua gestão e governança, se torna possível avançar na análise. Para tal, é preciso entender o que são dados marítimos compartilhados e como é feita a sua governança. Os dados marítimos compartilhados são, em sua grande maioria, dados logísticos sobre as embarcações e a carga transportada. Dentro da realidade brasileira é possível citar o programa para o Sistema de Gerenciamento da Amazônia Azul (SisGAAz) como exemplo de sistema para a geração e compilação de informações sobre o tráfego marítimo estabelecido pela Autoridade Marítima. Ele será composto por diversos radares, câmeras e outros sistemas que coletarão os dados de tráfego e auxiliarão na garantia da segurança das águas jurisdicionais brasileiras.[17]

Dentre esses outros sistemas figura o Sistema de Monitoramento Marítimo de Apoio às Atividades de Petróleo (SIMMAP), o Sistema de Identificação e Acompanhamento de Navios a Longa Distância (LRIT), o Programa Nacional de Rastreamento de Embarcações Pesqueiras por Satélite (PREPS) e o Sistema de Informação Sobre o Tráfego Marítimo (SISTRAM). Este último também utiliza o processamento de dados eletrônicos para realizar o acompanhamento dos navios mercantes tanto em águas interiores como em rotas de longo curso.

O VTS e o VTMIS, cuja implementação nos portos brasileiros é regulada pela NORMAM 26, contribuem como fonte de dados de tráfego marítimo a serem compartilhados. Eles são “sistemas em terra que variam desde o fornecimento de mensagens simples de informação aos navios, como a posição de outro tráfego ou avisos de perigo meteorológico, até a gestão extensiva do tráfego dentro de um porto ou via navegável”. (INTERNATIONAL MARITIME ORGANIZATION, S.A, *apud* Relatório de Pesquisa Logística Marítima e a Importância do VTMIS, p.31). Alguns dos equipamentos utilizados por essas tecnologias são radares, AIS, Comunicações VHF, TV de circuito fechado (CCTV), sensores meteorológicos e ambientais.

Diferentes agências governamentais podem fazer uso dessas informações para realizar suas atividades de controle e regulação dentro dos portos organizados ou instalações portuárias privadas. A ANTAQ, o IBAMA, a ANVISA e a Polícia Federal são exemplos de algumas dessas agências. No relatório “Compartilhamento e Integração de Informações do Movimento Marítimo: uma abordagem para o desenvolvimento do cluster tecnológico naval do Rio de Janeiro", produto da parceria entre a Fundação EZUTE e a Escola de Guerra Naval, expõe-se a

importância da integração e cooperação no compartilhamento dessas informações entre os entes dentro dos clusters. Os principais resultados são a diminuição dos custos e a otimização da produção e dos serviços dentro dos portos.

A governança deste tipo de informação é de extrema importância para o bom funcionamento do porto. A *European Union Agency for Cybersecurity* (ENISA, 2019) aponta em seu relatório diversas ameaças à segurança que podem ocorrer com o vazamento deste tipo de informação. Há a possibilidade de, por exemplo, agentes mal-intencionados invadirem os sistemas e isso causar uma pausa nas operações portuárias. Ou até mesmo haver identificação de cargas mais valiosas para futuro roubo delas. Sendo assim, se faz necessário o controle de quem tem acesso às informações e como as obtêm. No caso do Brasil há uma hierarquização das informações e níveis de acesso. Imagens do tráfego (radar), câmera de segurança e comunicação por voz são de caráter sigiloso. Já dados de meteorologia e hidrografia, programação de atracação, registro de manobras, documentos de auxílio a navegação e outros mais são classificados como ostensivos. A Marinha do Brasil, a ANTAQ, a Polícia Federal e a Receita Federal possuem interesse e acesso às informações de caráter sigiloso e não sigiloso, já atores como a Praticagem do Brasil possuem interesse nos dados não sigilosos (VILLAS-BÔAS, 2020 *apud* Relatório de pesquisa Compartilhamento e Integração de Informações do Movimento Marítimo, p. 36).

A seguir, o presente relatório apresentará uma análise do modelo de gerenciamento de dados do tráfego marítimo compartilhado dos principais portos da região Sudeste do Brasil. Desta forma será possível compreender como tal compartilhamento de dados ocorre na prática dentro dos portos brasileiros. Para determinar quais portos fariam parte da análise, realizou-se um levantamento de dados relacionados à movimentação de carga dos portos do Sudeste, em tonelada e em TEU, na base do anuário da ANTAQ.

Foram selecionados então os portos com maior movimentação de carga, visto que a própria agência utiliza esse mesmo parâmetro por permitir identificar a participação de cada porto no comércio brasileiro. Este relatório trabalhará com os seguintes portos: i) Santos; ii) Vitória; iii) Itaguaí; iv) Porto do Açu e; v) Rio de Janeiro[18]. As figuras 2 e 3 ilustram gráficos que mostram o volume de movimentação, em toneladas, dos portos em 2022 (contando apenas os meses de janeiro a julho) e 2021 respectivamente.

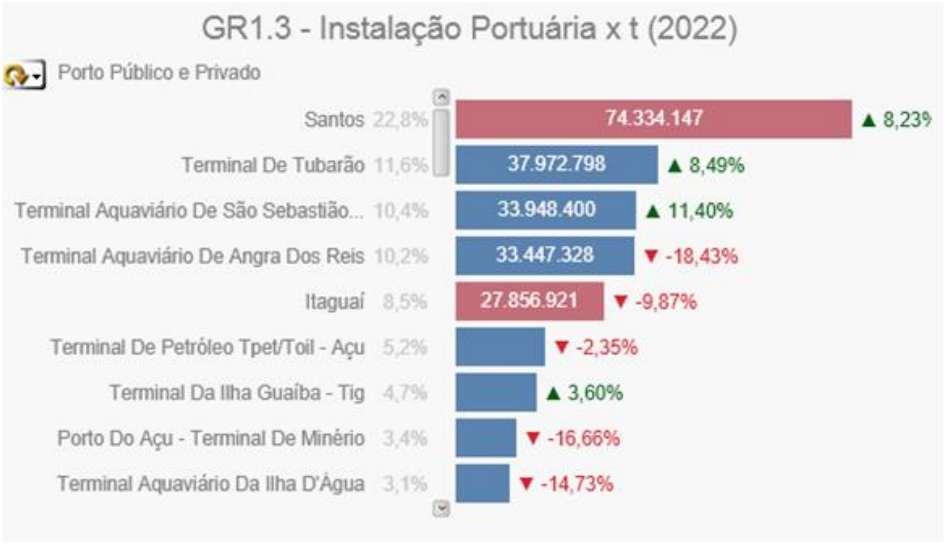

Figura 2- Principais Portos do Sudeste em movimentação de granel (2022)
Fonte: Painel Estatístico Aquaviário da ANTAQ

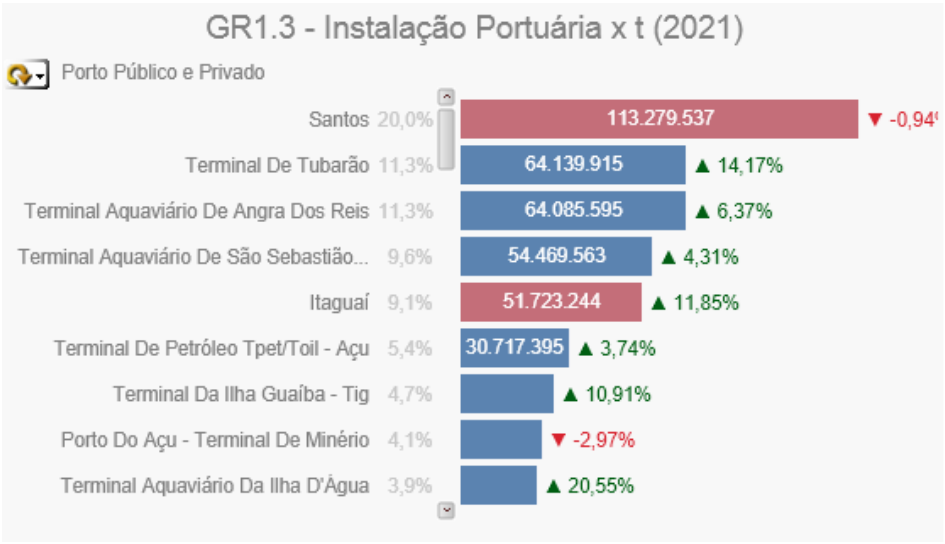

Figura 3- Principais Portos do Sudeste em movimentação de granel (2021)
Fonte: Painel Estatístico Aquaviário da ANTAQ

O Brasil é um país que movimenta cargas pesadas, tanto em 2021 quanto em 2022 foram os granéis sólidos, principalmente o minério de ferro, que ocuparam o segundo lugar do grupo de mercadorias mais movimentadas. O primeiro foi o dos combustíveis e óleos minerais e produtos da sua destilação. Sendo assim, a análise da movimentação dos portos será feita a partir do volume de unidades de contêineres movimentadas.

Há uma pequena diferença na classificação dos portos quando se faz a observação da movimentação a partir dos contêineres. Do mais movimentado para o menos movimentado, são eles: i) Santos; ii) Rio de Janeiro; iii) Vitória e; iv) Itaguaí. Como é possível perceber, o Porto do Açu não figura entre os principais portos que movimentam cargas conteinerizadas. Além disso, o Porto do Rio de Janeiro, que antes ocupava a última posição, passa a ser o segundo mais movimentado. Essas constatações podem ser depreendidas da leitura dos gráficos ilustrados nas figuras 4 e 5.

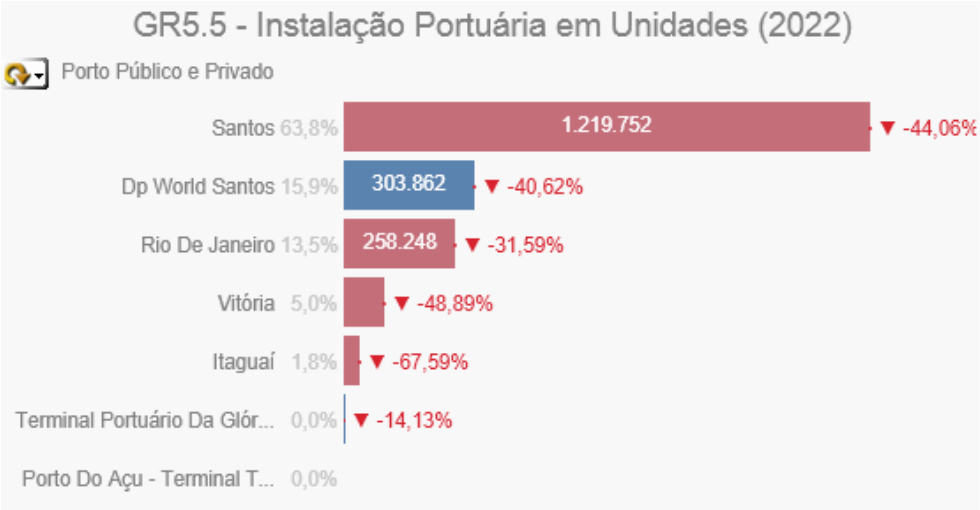

Figura 4- Principais Portos do Sudeste em movimentação de contêiner (2022)
Fonte: Painel Estatístico Aquaviário da ANTAQ

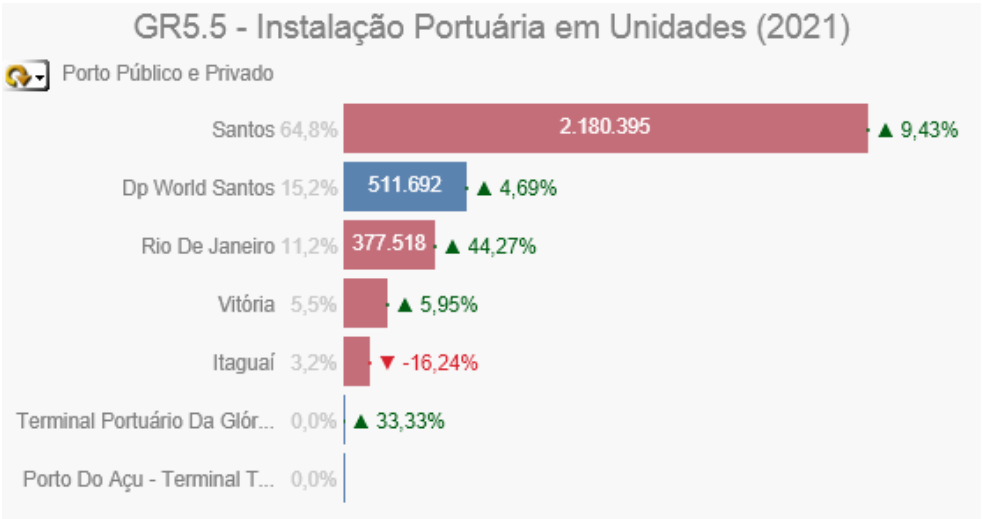

Figura 5- Principais Portos do Sudeste em movimentação de contêiner (2021)
Fonte: Painel Estatístico Aquaviário da ANTAQ

4.1 ANÁLISE DO MODELO DE GERENCIAMENTO DE DADOS DOS PRINCIPAIS PORTOS DA REGIÃO SUDESTE

4.1.1 Porto do Açu

O Porto do Açu, localizado no município de São João da Barra (RJ), iniciou suas operações em 2014. Ocupando uma área total de 130 km², o porto é composto por 9 terminais divididos em áreas *onshore* e *offshore*. A empresa Prumo Logística, afiliada ao Porto de Antuérpia e Bruges, é a autorizatária para explorar o porto, contando com parcerias de outras empresas para a gestão dos terminais.[19]

Em 3 de dezembro de 2015, através da portaria de nº 208, o porto adquiriu a licença para a operação do VTS[20]. Compete então à Porto do Açu Operações SA a administração do Centro VTS do Açu, autoridade VTS estabelecida junto à Autoridade Marítima.[21] O centro é composto pelas seguintes tecnologias: RADAR Banda-X; Estação Base AIS classe "A"; Transceptor VHF; Circuito fechado de TV - CCTV; Estação meteoceanográfica; e Sistema de gerenciamento do tráfego *Navi Harbour*.[22] Essas tecnologias são integradas a outros sistemas, como o *Port Management Information System.* Atualmente, o serviço prestado pelo porto é o de INS (serviço de informação), tipo mais básico de VTS.

A gestão de riscos dentro do Porto do Açu é feita através de planos de ação atualizados anualmente. São levados em conta os riscos operacionais, estratégicos, financeiros, de conformidade/legais e reputacionais. O porto se baseia na ISO 31000 e no COSO *Enterprise Risk Management* para a criação de seus planos de gerenciamento.[23] Além disso, com uma cultura que tem a segurança como valor, o Programa de Integridade funciona como ferramenta de governança e de padronização comportamental de seus colaboradores. Não foram encontrados, no âmbito desta pesquisa, nenhum plano de desenvolvimento e zoneamento para o porto em questão.

O Porto do Açu, na versão mais recente de seu regulamento portuário [24] e na cartilha de procedimentos para os navegantes na área de VTS[25], deixa claro a sua preocupação com os dados de tráfego marítimos compartilhados. Consta no regulamento supracitado que o Centro VTS tem o poder de:

> (ii) Trocar informações de caráter náutico, afeto à segurança da navegação, entre Terminais, Embarcações, Práticos, Rebocadores, Serviços Aliados e Autoridades Competentes; (...) (v) Registrar, processar, arquivar e disponibilizar informações adquiridas pelos seus equipamentos às Autoridades Competentes e/ou outras partes interessadas." (PORTO DO AÇU, 2019, p.23).

Além disso, as informações coletadas pelo Centro VTS poderão ser compartilhadas com as autoridades sempre que solicitado. Entretanto, o compartilhamento com "partes interessadas" fica a critério da administração portuária que poderá liberar, ou não, tais informações com ou sem custo a partir da análise de uma solicitação oficial.

Entretanto, riscos cibernéticos não foram considerados de forma específica na lista de disposições para prevenção de danos e acidentes, não foram encontradas nas regulações supracitadas medidas de segurança específicas para a proteção desses dados e/ou para o seu compartilhamento. É possível perceber que o mesmo fenômeno acontece nas listas de comportamentos proibidos, nenhum deles trata de forma específica de ameaças à segurança cibernética. Além disso, nem mesmo no documento de Política de Governança Corporativa [26] constam diretrizes específicas quanto ao comportamento virtual dos usuários e colaboradores da empresa.

4.1.2 Porto do Rio

O Porto do Rio de Janeiro é um porto público que tem como Autoridade Portuária a Companhia Docas do Rio de Janeiro (CDRJ), responsável pela gestão de todos os portos públicos do estado do Rio de Janeiro) (AUTORIDADE PORTUÁRIA DO RIO DE JANEIRO, S.A).

Em termos históricos, apesar do Rio de Janeiro ser encimada como capital do Brasil em 1763, sendo um dos principais pilares econômicos do país na movimentação de ouro proveniente da região das Minas e do tráfico de escravizados, a atual localização deste porto foi inaugurada oficialmente em 20 de julho de 1910. Antes dessa inauguração, na época do Brasil Imperial, 50 anos antes da inauguração, na década de 1870 foram elaborados os primeiros projetos de desenvolvimento portuário do Rio de Janeiro. Em tais projetos, o foco era unificar as instalações portuárias que até então eram dispersas em regiões distintas da cidade como: Estrada de Ferro Central do Brasil, da Ilha dos Ferreiros, da Enseada de São Cristóvão, da Praça Mauá, além dos cais Dom Pedro II, da Saúde, do Moinho Inglês e da Gamboa. No ano de 1890, um ano depois da Proclamação da República, autorizou-se por meio de decretos[28] a construção de" um conjunto de cais acostáveis, armazéns e alpendres. Foram escolhidos os trechos entre a Ilha das Cobras e o Arsenal de Marinha, e do Arsenal de Marinha até a Ponta do Caju" pelas empresas Industrial de Melhoramentos do Brasil e *The Rio de Janeiro Harbour and Docks* (COMPANHIA DE DOCAS DO RIO DE JANEIRO, S.A.[29]).

Ao longo dos anos o porto mudou de autoridade portuária, até que na década de 1930 foi constituído porto federal autônomo. Apenas em 9 de julho de 1973, por meio do decreto n° 72.439 que a Companhia de Docas da Guanabara foi criada, sendo este o atual CDRJ.

Localizado na costa oeste da baía de Guanabara, o porto do Rio de Janeiro, de acordo com o documento Desenvolvimento e Integração Porto-Cidade de 2020, tem uma posição estratégica "e a oferta de infraestruturas logísticas, presentes de norte a sul do Estado do Rio de Janeiro, fazem com que, por seus terminais, sejam movimentadas cargas com origem ou destino a diferentes unidades federativas" (COMPANHIA DE DOCAS DO RIO DE JANEIRO, S.A.[30]).

Segundo a CDRJ, atualmente, o Porto do Rio trabalha com os seguintes tipos de carga: produtos siderúrgicos, ferro gusa, carga geral, carga conteinerizada, trigo, concentrado de zinco, cargas de apoio offshore e com uma variedade de granéis líquidos e sólidos (COMPANHIA DE DOCAS DO RIO DE JANEIRO, S.A.).

Após este apanhado histórico e geográfico, é importante voltar ao escopo deste relatório que trata sobre governança e gerenciamento de dados de tráfego marítimo. Segundo o último Plano de Desenvolvimento e Zoneamento Portuário (PDZ) do Porto do Rio de Janeiro, datado de 2016, o sistema de controle e monitoramento de tráfego marítimo que é instrumentalizado no porto é o *Automatic Identification System* (AIS) que consiste em:

> [...] um sistema de monitoração de longo alcance utilizado em navios e serviços de tráfego de embarcações. O AIS integra um sistema transceptor VHF, servindo para identificar e localizar embarcações por intermédio da troca eletrônica de dados com outros navios e estações AIS. Informações tais como identificação, posição, curso e velocidade são exibidas em uma tela e acompanhadas 24h pelos técnicos plantonistas (COMPANHIA DE DOCAS DO RIO DE JANEIRO, 2016, p.87.).

A CDRJ no PDZ de 2016 elencou os principais pontos de melhoria operacionais que estavam sendo planejadas ou feitas no porto do Rio, no caso dos sistemas de monitoramento e controle de dados de tráfego marítimo como o VTS e VTMIS, o porto estava com suas respectivas implantações paralisadas. Apesar do PDZ ser de 2016, em 2021 o projeto deu prosseguimento com a CDRJ adquirindo equipamentos para a implantação de um Local Port Service [8](LPS) nos portos do RJ e de Niterói até o final deste ano, 2022.

[8] A Local Port Service is applicable to those ports where it has been identified from their Formal Safety Assessment that a VTS is excessive or inappropriate. They will not, therefore, be required to train their operators to the V-103 standard. [...] the main difference arising from the provision of LPS is that it does not require to have the ability and / or the resources to respond to developing traffic situations and there is no requirement for a vessel traffic image to be maintained. As such, the equipment fit does not need to be as extensive as for a VTS, the training requirement for its operators is less comprehensive and the operators do not need to be certified to the V-103

O projeto de implantação do VTMIS no porto do Rio de Janeiro ocorre de forma escalonada, seguindo a ordem de implantação: i) LPS; ii) VTS e depois; iii) VTMIS, sendo a primeira vez que um VTMIS é implantado de tal forma. Segue abaixo a função de cada um dos projetos implantados ou a serem implantados:

Figura 6- Ordem de implantação do VTMIS do Porto do Rio de Janeiro
Fonte: VILLAS BOAS; BRIGLIA E VIDAL 2021.

.

4.1.3 Porto de Itaguaí

No dia 07 de maio de 1982 foi fundado na costa norte da Baía de Sepetiba o Porto de Itaguaí. Assim como os demais portos públicos situados no estado do Rio de Janeiro, Itaguaí é gerido pela CDRJ, possuindo cerca de 7,2 mil km² de infraestrutura voltada para a movimentação de cargas como contêineres, minérios, outros granéis sólidos, produtos siderúrgicos e carga geral.

Segundo o Plano de Desenvolvimento e Zoneamento Portuário (PDZ) do Porto de Itaguaí datado de 2019, a área que constitui o porto organizado de Itaguaí foi estabelecida em 10 de maio de 2007 pelo então Presidente da República, tendo:

> [...] instalações portuárias terrestres, tais como: cais; píeres de atracação; armazéns; pátios; edificações em geral; vias, passeios e terrenos ao longo das faixas marginais abrangidos pela poligonal caracterizadora da área definida no próprio decreto; e pela infraestrutura de proteção e de acessos aquaviários – que compreende o canal de acesso, as áreas de fundeio e as bacias de evolução (COMPANHIA DOCAS DO RIO DE JANEIRO, 2019, p. 2).

Tendo em vista que a Autoridade Portuária de Itaguaí é a mesma do Porto do Rio, ambos usam o mesmo sistema de monitoramento do tráfego aquaviário, o AIS que “consiste em um

standard. Acesso em: https://www.gov.uk/government/publications/mgn-401-mf-amendment-3-navigation-vessel-traffic-services-vts-and-local-port-services-lps-in-the-uk/mgn-401-mf-amendment-3-navigation-vessel-traffic-services-vts-and-local-port-services-lps-in-the-uk#local-port-services-lps

sistema de monitoração de curto alcance utilizado em navios e serviços de tráfego de embarcações" (COMPANHIA DOCAS DO RIO DE JANEIRO, 2019, p. 47). Vale ressaltar que o AIS integra um sistema transceptor VHF, servindo "para identificar e localizar embarcações por intermédio da troca eletrônica de dados com outros navios e estações AIS. Informações tais como identificação, posição, curso e velocidade são exibidas em uma tela e acompanhadas 24 horas pelos técnicos plantonistas" (COMPANHIA DOCAS DO RIO DE JANEIRO, 2019, p. 47).

Dessa forma, assim como no Porto do Rio de Janeiro, Itaguaí não possui VTS/VTMIS, estando em fase de elaboração do Projeto Básico do VTMIS. Tendo em vista a correlação das autoridades portuárias e o fato do PDZ de Itaguaí ser de 2019 e o do Rio de 2016, é possível inferir que ambos possuem status similares de implantação do VTS.

4.1.4 Porto de Santos

O Porto de Santos está localizado no estuário de Santos, limite natural entre os municípios de Santos, Guarujá e Cubatão. Composto por um conjunto de 53 terminais usados tanto para armazenagem quanto para movimentação de cargas e passageiros, o porto é público e administrado pela União através da Autoridade Portuária de Santos S.A.

A área terrestre do porto compreende 8 km², já a infraestrutura aquaviária está contida em uma área de cerca de 355,5 km².[33] O porto contém um plano de zoneamento e desenvolvimento (PDZ) publicado em 2020 com previsões de expansão das operações até 2040 (AUTORIDADE PORTUÁRIA DE SANTOS, 2020).

O sistema VTMIS ainda está em fase de implantação. Em dezembro de 2021 o porto estabeleceu uma parceria com a Fundação Ezute para elaboração do projeto básico para a implantação do sistema de gerenciamento de informações do tráfego de embarcações.[34] Em dezembro de 2022 a Fundação entregou o projeto básico com os estudos de viabilidade, atividades de engenharia de sistemas e definição de requisitos consolidados.[35] No PDZ lançado em 2020 já constam algumas diretrizes sobre a gestão dos dados de tráfego marítimo. Destaca-se que todo tráfego deverá seguir as diretrizes que constam na NORMAM – 08 da Autoridade Marítima para tráfego e permanência de embarcações em águas jurisdicionais brasileiras.

A governança no Porto de Santos é feita através de normas, manuais e canais de comunicação. Dentre alguns exemplos é possível citar o Estatuto Social, a ouvidoria, as normas da autoridade portuária e o conjunto de políticas da empresa.

No plano estratégico do porto para os anos de 2021 a 2025 é possível enxergar um esforço da autoridade portuária de entender as fraquezas de sua administração e possíveis ameaças ao porto. Além disso, é possível conferir também alguns planos de ação para solucionar problemas eminentes.

A cyber segurança já é uma questão que recebe atenção da Autoridade Portuária de Santos. No plano estratégico supracitado os ataques cibernéticos são listados como possível ameaça ao porto, sendo a busca pela certificação ISO 27001 a medida divulgada pela administração portuária para dirimir a questão. Foram listadas também outras medidas referentes a segurança das operações e transformação digital[37]. Além disso, o porto também possui um manual do Sistema de Gestão de Segurança e Privacidade da Informação (SGPI), o que mais uma vez demonstra a sua preocupação com a segurança dos dados e de seu compartilhamento[38].

4.1.5 Porto de Vitória

O Porto de Vitória é um porto público administrado pela CODESA (Companhia Docas do Espírito Santo). Sua área, definida na Portaria nº 4-2021 do Diário Oficial da União, é de aproximadamente 139 km². Inaugurado em 1940, o porto está localizado parte no município de Vitória e parte no município de Vila Velha.

No PDZ lançado em 2017 é possível conferir todo o histórico de desenvolvimento do porto juntamente com todos os marcos legais que o acompanham[39]. Em março de 2022, o Fundo de Investimentos em Participações Shelf, liderado pela Quadra Capital, venceu o leilão de privatização da Companhia Docas do Espírito Santo na Bolsa de Valores de São Paulo, por R$ 106 milhões de outorga, com um contrato de concessão de 35 anos, prorrogáveis por mais cinco[9].

O sistema VTS está em funcionamento no porto desde 04 de setembro de 2017.[40] No documento “Procedimentos para os Navegantes”, o porto informa que os dados de tráfego uma vez solicitados serão compartilhados, não demonstrando assim uma maior preocupação quanto a possíveis vulnerabilidades decorrentes do processo.

Em novembro de 2022 o centro de operações do VTS do Porto de Vitória recebeu a visita de oficiais da Marinha do Brasil para a verificação do seu bom funcionamento, incluindo questões relacionadas à segurança cibernética.

[9] https://www.cnnbrasil.com.br/business/fundo-arremata-codesa-por-r-106-milhoes-em-1a-privatizacao-portuaria-do-pais/

No plano de desenvolvimento e zoneamento do Porto de Vitória constam algumas medidas de segurança, inclusive cibernética, tomadas por alguns terminais que o compõe. Mas nada é dito em específico sobre as medidas da autoridade portuária quanto a segurança cibernética dos dados portuários.

5 SEGURANÇA CIBERNÉTICA DOS DADOS DE TRÁFEGO MARÍTIMO

Em novembro de 2019, a *European Union Agency for Cybersecurity* (ENISA) publicou o relatório "*Port Security: Good Practices for Cybersecurity in the Maritime Sector*" que visa a apresentar os principais desafios e a evolução na área de cibersegurança nos portos europeus. Este estudo objetivou construir um compilado de boas práticas de segurança cibernética dos portos europeus, mapeando desafios e ameaças, destacando cenários de ataque, a fim de promover uma colaboração no ecossistema marítimo e portuário da União Europeia (UE) (ENISA, 2019).

Este capítulo será segmentado em três partes: Na primeira delas, as proposições elaboradas pela ENISA no contexto europeu com a finalidade de salvaguardar o ecossistema marítimo e portuário no que tange a cibersegurança serão apresentadas. Logo em seguida, o relatório apresentará as medidas já em vigor nos principais portos da região sudeste do Brasil. E por fim, as algumas sugestões de melhoria aos modelos brasileiros com base nas concepções feitas pela agência europeia serão propostas.

5.1 Proposições da ENISA

A Agência para Segurança Cibernética da União Europeia, no relatório sobre segurança nos portos publicado em 2019, elencou algumas medidas de segurança que podem ser incluídas e/ou intensificadas nos portos europeus. O objetivo desta seção é expor estas medidas para que, na próxima seção, seja analisado o quão aplicáveis elas são à realidade brasileira. A organização dividiu suas proposições em três grandes grupos: políticas, práticas organizacionais e práticas técnicas.

5.1.1 Políticas Organizacionais

As primeiras proposições são as políticas, segundo a ENISA é essencial que os complexos portuários estabeleçam políticas regulatórias e governança em matéria de Tecnologia da Informação (TI) e Tecnologia de Operação (TO), com a finalidade de aplicar as melhores práticas na área da cibersegurança, dando um enfoque nos bens mais críticos da infraestrutura portuária, baseando-se em uma abordagem de risco. As proposições políticas da ENISA são divididas nas seguintes categorias:

i) Política de segurança e organização;
ii) Gerenciamento de riscos e ameaças;
iii) Projetos de segurança e privacidade;

iv) Inventário e Gestão de Ativos; e

v) Resiliência cibernética.

Cada uma dessas categorias propositivas visa a garantir a integridade cibernética dos portos europeus (ENISA, 2016).

As Políticas de segurança e organização tem o objetivo de criar medidas de segurança que implementem e atualizem constantemente a política de segurança da informação de determinado porto. Dessa forma, o esforço feito é escrever e implementar informações e boas práticas na política de sistemas de segurança, a fim de descrever as medidas e procedimentos técnicos e organizacionais que devem ser seguidos por todos os colaboradores e stakeholders do complexo portuário. Após a elaboração desta política, é necessária aprovação das medidas pelo mais alto escalão de gestores. Além de elaborar um documento procedimental com práticas que garantem a segurança da infraestrutura portuária, a política de segurança e organização também busca o cumprimento da governança da segurança dos ambientes informáticos e de TO. Para isso, descreve-se os papéis e responsabilidades de cada stakeholder, seja ele interno (Autoridade Portuária e terminais) ou externo (fornecedores e autoridades federais). Consequentemente, todas essas recomendações e práticas precisam ser compartilhadas com todos os envolvidos na operação portuária, visando ao engajamento e segurança de todos. Esta política de segurança dos sistemas de informações (ISSP, sigla em inglês) precisa ser revista anualmente, considerando as novas ameaças e riscos que surgem devido às inovações tecnológicas, mas também devido aos mapeamentos e análises de riscos (ENISA, 2016).

A segunda categoria é o gerenciamento de riscos e ameaças que consiste na elaboração de medidas na área de segurança por parte do porto, que visam a identificar, relatar e gerir de forma contínua os possíveis riscos e ameaças ao ecossistema portuário (ENISA, 2016).

Para alcançar tal fim é necessário que o porto adote uma abordagem lastreada na detecção do risco, a fim de construir uma estratégia de segurança cibernética portuária, estabelecendo "um processo de melhoria contínua para garantir que os riscos identificados estejam sob controle e que novos riscos sejam devidamente identificados de forma oportuna" (ENISA, 2016, p. 40, tradução nossa).

Além disso, a ENISA reforça que um bom gerenciamento de riscos e ameaças em estruturas portuárias trazem os seguintes resultados: i) assegura que os riscos cibernéticos sejam identificados e alinhados com os programas de segurança e integridade física do porto; ii) conduzem e criam a prática de identificar riscos e analisá-los, principalmente no escopo de

novos projetos; iii) estabelecem novos métodos de segurança, de avaliação, monitora-se novos indicadores e processos, a fim de acompanhar o desempenho da gestão de riscos, envolvendo todos os stakeholders portuários e; iv) estabelece um processo de inteligência e gestão de ameaças em que se mapeia constantemente as possíveis ameaças e riscos, elaborando-se ações e esforços para mitigá-los.

É interessante frisar que no caso europeu a ENISA pontua que o quarto resultado citado pode ser melhorado através do desenvolvimento conjunto de iniciativas cooperativas e colaborativas entre órgãos públicos e privados no que tange o compartilhamento de informações sobre inteligência de ameaças a nível europeu (ENISA, 2016).

A terceira categoria de proposições da ENISA, são os projetos de segurança e privacidade, essa categoria pode ser conceituada como medidas de segurança que precisam ser aplicadas e implementadas de forma embrionária "desde as primeiras etapas do desenvolvimento de sistemas e durante o ciclo de vida do desenvolvimento, a fim de aumentar, através do projeto, os níveis de segurança de quaisquer soluções" e aplicações, protegendo dados críticos/sensíveis e garantindo a privacidade dos dados pessoais e portuários (ENISA, 2016, p. , tradução nossa).

Com a finalidade de tangibilizar a realização dos projetos de segurança e privacidade, a ENISA elenca três ações que são necessárias. A primeira consiste no desenvolvimento de uma metodologia de gestão de projetos, focada em avaliações de segurança, pontos de controle, utilizando-se análise de risco, revisão da arquitetura de segurança, testes de segurança, simulações, entre outros, inclusive em projetos ágeis. A ideia disseminada por este ponto é garantir que em todos os projetos portuários, desde sua concepção até as fases de implantação e monitoramento, as questões de segurança cibernética sejam vistas e bem tratadas (ENISA, 2016).

A segunda ação recomendada é que se aborde e se respeite em todos os processos, políticas e regulamentos internos e as questões relacionadas à legislação local e internacional sobre a gestão do uso de dados. No documento, a ENISA cita o Regulamento Geral de Proteção de Dados (GDPR) no caso europeu. Pensando no Brasil, deve-se trabalhar neste ponto com a centralidade da Lei Geral de Proteção de Dados. Trabalhar com a legislação local e internacional não é apenas uma questão legal, mas também securitária, tendo em vista que a criação de tais leis é espelhada em práticas, ameaças e técnicas observadas internamente em diversos portos.

A terceira e última ação é a elaboração de um projeto de classificação dos dados com a finalidade de identificar quais são os dados críticos para as operações portuárias. Este processo consiste em ordenar quais dados são essenciais, quais são sensíveis, sendo estes os que precisam de mais proteção e quais dados são públicos (ENISA, 2016).

Os dois últimos grupos de proposições políticas da ENISA são o inventário e a gestão de ativos, que são "medidas de segurança relativas ao mapeamento do ecossistema, incluindo ativos dos portos e ativos de terceiros interagindo com os ativos portuários" (ENISA, 2016, tradução nossa), e a resiliência cibernética, que são "medidas de segurança estabelecidas para garantir, em caso de qualquer incidente, ou pior, desastre, a continuidade de operações portuárias e recuperar dados" (ENISA, 2016, tradução nossa). Em ambas as proposições a ENISA define 3 ações, no caso do inventário e gestão de ativos é necessário softwares de gestão, após a contratação do software e de toda a infraestrutura que o compõe e o protege, deve-se criar uma política para uso dessa ferramenta, elencando quem pode ou não a usar. Além disso, deve-se criar ferramentas centralizadas que monitorem os diferentes ativos do porto.

Finalizando as ações políticas, no caso da resiliência cibernética, a ENISA propõe que se deve garantir a resiliência cibernética dos sistemas portuários definindo objetivos, estratégias, e parâmetros importantes que visem à continuidade do negócio caso haja uma crise ou desastre, definindo assim os pontos a serem recuperados. Além disso, é necessário definir um processo de gerenciamento de crise global a toda infraestrutura portuária, tendo treinamentos, políticas e regulamentos internos, sendo também necessário garantir a eficiência dos procedimentos de recuperação de todas as áreas e *stakeholders* portuários.

5.1.2 Práticas Organizacionais

As práticas organizacionais devem fazer parte do dia a dia dos colaboradores do porto de forma a garantir a segurança das TI e das TO. O primeiro conjunto de práticas diz respeito a atenção aos ciclos de vida e proteção dos dispositivos finais como *desktops*, celulares, *notebooks e tablets*. É interessante que se defina uma estratégia de segurança para essas tecnologias envolvendo meios físicos e *softwares* como programas antivírus e criptografia. Construir uma lista de dispositivos e programas permitidos para uso que seja constantemente revista também colabora para a manutenção da segurança. Além disso, é preciso definir protocolos para uso e incorporação de novos dispositivos à rede portuária e reforçar com os colaboradores que aqueles dispositivos cuja utilização foi suspensa não pode ser descartado sem antes passar por processos de limpeza de dados.

Em seguida o relatório passa a falar sobre as práticas organizacionais que envolvem vulnerabilidades. Em primeiro lugar é recomendado que se estabeleça um processo, seja ele manual ou automático, de identificação das vulnerabilidades. Para que então sejam estabelecidos processos de segurança cibernética direcionados a elas e que estes, sejam adotados e expandidos para todos os *stakeholders* envolvidos.

Dentre as práticas organizacionais também estão inclusos os recursos humanos. Intensificar as pesquisas por referências profissionais e históricos criminais dos colaboradores portuários também são medidas de segurança. Juntamente com a ministração de cursos obrigatórios e o desenvolvimento de uma cultura voltada para a segurança cibernética e as principais ameaças que a envolvem.

A administração dos processos de *supply chain* é importante justamente por requerer medidas de proteção no contato com terceiros. Para isso, deve-se restringir o acesso destes prestadores de serviço ao sistema portuário ao máximo, de forma que suas operações se limitem ao estritamente necessário durante um certo período. Além disso, é preciso que as medidas de segurança constem nos contratos e acordos de prestação de serviço.

O relatório também chama a atenção para algumas práticas organizacionais que envolvem a definição de processos de identificação e resposta a incidentes no sistema portuário. A primeira medida deve ser a de detectar riscos e ameaças em todo o porto e, a partir disso, elencá-los de acordo com seu nível de impacto. Assim será possível estabelecer políticas e procedimentos para identificação e resposta a incidentes, além de implementação de padrões de comunicação das ameaças para todos os *stakeholders* e colaboradores do porto. Uma vez implementados, deve-se constantemente buscar melhorias e atualizações desses processos. É importante que, tanto o porto quanto seus *stakeholders*, considerem a criação de um Centro de Operações de Segurança Cibernética que sejam coordenados entre si e definam procedimentos padrão para a emissão de alertas de incidentes e sua criticidade.

Boas práticas de segurança e *compliance* são igualmente mencionadas pela ENISA. Realizar auditorias regulares de segurança cibernética para identificar a efetividade das medidas implementadas e rever periodicamente as regras de navegação na rede do porto, incluindo os controles de acesso, é de extrema importância.

Por fim, o último conjunto de práticas organizacionais para a segurança portuária diz respeito à proteção física das TI e TO. Deve-se intensificar as boas práticas de segurança, virtual e física, dos sistemas em operação e rastrear todos os processos de manutenção realizados.

5.1.3 Medidas Técnicas

Outra categoria de proposições citada pela organização europeia se refere às medidas técnicas, cuja importância está diretamente relacionada à detecção, prevenção, resposta e redução de impactos dos ataques cibernéticos.

As informações, arquivos e dados guardados em nuvens também devem ser protegidos. Para tal, a ENISA recomenda definir um método de avaliação da segurança nesses espaços e em seu uso. Incluir cláusulas de segurança nos contratos com os provedores das nuvens. E, na medida do possível, considerar a nuvem ao criar e implementar medidas de detecção e de resposta a ameaças.

Deve-se também se preocupar com as trocas de informações entre as máquinas. Implementar mecanismos de segurança, promover autenticação mútua, encriptação dos dados compartilhados entre outras medidas de certificação são as soluções sugeridas. Além disso, é sugerido também que sejam implementados protocolos de comunicação que detectem caso uma mensagem, ou parte dela, não seja autorizada para compartilhamento.

Quanto à proteção de dados nos sistemas portuários, recomenda-se a implementação de criptografia e outros mecanismos para proteger informações confidenciais, de forma proporcional a sua sensibilidade, e a integridade do sistema portuário. Além disso, a organização europeia também recomenda que os dados pessoais processados pelo porto sejam tornados anônimos e com permissão de acesso de acordo com a função do colaborador.

Os sistemas utilizados no porto também devem estar sempre atualizados e para isso é preciso que sejam estabelecidos processos de administração das atualizações. As certificações de autenticação e a integridade das máquinas devem ser reforçadas, juntamente com a análise e controle sobre a atualização e verificação de sua fonte.

Os sistemas e dispositivos portuários devem ser muito bem monitorados e em tempo real. A instalação de sistemas de registro de usuários é importante para o rastreamento das atividades realizadas dentro dos sistemas pelos usuários. Além disso, eles também podem emitir alertas de ataque cibernético quando identificarem atividades suspeitas / incomuns.

A segurança dos sistemas de controle industrial está diretamente relacionada com as TO. A ENISA sugere que sejam consideradas todas as medidas de segurança aplicáveis mencionadas anteriormente. Caso isso não seja possível, é recomendado que se adote medidas compensatórias. Ademais, as redes de TI e TO devem ser segmentadas e, caso haja a utilização da internet das coisas (IoT), medidas de segurança específicas devem ser implementadas.

Por fim, as últimas sugestões feitas pela organização europeia giram em torno dos processos de *backup* de dados e restauração. Com atenção especial a dados e sistemas críticos, a utilização de *backups* irá facilitar a recuperação de possíveis dados perdidos durante um ataque cibernético.

5.2 Arcabouço documental portuário brasileiro

Serão apresentadas duas legislações que norteiam a estruturação dos portos brasileiros, a Lei dos Portos (Lei 12.815/2013) e a portaria nº 61 do Ministério da Infraestrutura. De antemão, vale ressaltar que nenhum dos documentos faz menção direta à segurança cibernética. Mas a análise deles se faz interessante justamente para entender melhor como a questão poderia ser abordada e em que parágrafos ela poderia ser incluída.

5.2.1 Portaria nº 61 do Ministério da Infraestrutura

É através desta portaria que o governo federal regula o planejamento da organização física dos portos. Sendo assim, logo no artigo 2º são definidos os termos plano mestre (PM), plano de desenvolvimento e zoneamento (PDZ) e plano geral de outorgas (PGO). Conforme consta no Diário Oficial da União,

> I - Plano Mestre (PM) - instrumento de planejamento de Estado voltado aos complexos portuários que abranjam os portos organizados, considerando as perspectivas do planejamento de transportes em nível estratégico, que visa a direcionar ações e investimentos de curto, médio e longo prazos nos portos, na relação porto-cidade e em seus acessos; II - Plano de Desenvolvimento e Zoneamento (PDZ) - instrumento de planejamento da Autoridade Portuária, que contempla as estratégias e ações para a expansão e o desenvolvimento integrado, ordenado e sustentável das áreas e instalações do porto organizado; e III – Plano Geral de Outorgas (PGO) - instrumento de planejamento de Estado, aderente às diretrizes do planejamento nacional de transportes, aos planos mestres e aos PDZ, com a finalidade de orientar investidores e consolidar projetos de outorga do setor portuário (Portaria nº61, art. 2º).

Ou seja, o plano mestre atua como um guia de para onde se pretende levar o porto, qual estrutura pretende-se alcançar. Sendo assim, é de sua competência:

> I – Projetar a demanda e a capacidade de atendimento das movimentações portuárias no horizonte do planejamento, e, também, aquelas dos acessos terrestres e aquaviários ao porto, tendo caráter orientativo aos demais instrumentos de planejamento; e II – realizar a análise estratégica do porto, buscando sua inserção de forma harmoniosa no complexo portuário nacional com base nas suas vantagens competitivas (Portaria nº61, art. 5º).

Cabe então ao "poder concedente", que no caso dos portos brasileiros é a União, a elaboração e atualização dos planos mestres a cada quatro anos (Portaria nº61, art. 4º). Entretanto, a Autoridade Portuária deve participar do processo de confecção, não só fornecendo dados e informações, mas também apresentando propostas de modificações que podem, ou não, serem aceitas (Portaria nº61, art. 6º).

Como o plano mestre é o documento delimitador dos futuros investimentos dos portos, é interessante observar que deve partir dele as primeiras intenções de promover a segurança cibernética dentro de um porto. E essa promoção pode partir tanto da União, ente que produz o documento, quanto da própria autoridade portuária, que tem influência sobre a confecção do documento.

É o plano mestre também o documento norteador dos planos de desenvolvimento e zoneamento dos portos, também conhecidos como PDZs. Apesar de serem confeccionados pela Autoridade Portuária, estes documentos precisam ser submetidos à aprovação do governo federal através da Secretaria Nacional de Portos e Transportes Aquaviários do Ministério da Infraestrutura (Portaria nº61, art. 9º). Não há nenhuma menção na portaria nº61 de obrigatoriedade de publicização destes documentos.

De acordo com o publicado no Diário Oficial da União, os PDZs precisam seguir as seguintes diretrizes:

> I - promoção do desenvolvimento do porto; II - otimização do uso das áreas, das instalações e da infraestrutura do porto; III – a adequação das áreas e instalações do porto visando à eficiência das operações portuárias e dos acessos ao porto; IV - integração do porto com os modais de transporte terrestre; V - definição do ordenamento das áreas e instalações do porto conforme as estimativas de movimentação de cargas e passageiros; VI – o atendimento às políticas nacionais para o setor portuário, observando, no que couber, as demais políticas para o transporte de cargas, em especial as do transporte aquaviário, de desenvolvimento social, econômico e ambiental; VII – o atendimento às projeções de demanda, os cálculos de capacidade e o Plano de Ações e Investimentos estabelecidos no Plano Mestre; VIII – as alternativas para a expansão das atividades portuárias, por perfil de carga; e IX - observância aos licenciamentos ambientais (Portaria nº61, art. 10º).

A respeito de seu conteúdo, o plano de desenvolvimento e zoneamento de um porto deverá:

> I - conter previsão de planejamento para os horizontes de curto, médio e longo prazos, aderente ao respectivo Plano Mestre; II – propor o uso das áreas afetas e não afetas às operações portuárias, em especial, aquelas que se encontram sem utilização; III – contemplar melhorias operacionais e os investimentos portuários e de acessos propostos no Plano Mestre; IV – propor a realocação de instalações existentes quando tal medida seja necessária para a obtenção de ganhos operacionais à atividade portuária; e V – contemplar levantamentos e estudos relativos ao desenvolvimento e zoneamento portuário (Portaria nº61, art. 11º).

Vale ressaltar que a Lei dos Portos, em seu artigo 5º-B inciso II, delimita que os processos de arrendamento dentro da área do porto organizado devem ser condicionados ao PDZ. Ou seja, empresas privadas só poderão atuar dentro das estruturas do porto organizado se seus interesses estiverem alinhados com o que foi planejado pela União.

Quanto a periodicidade de atualização, o PDZ deve ser repensado em até no máximo um ano após a confecção de um novo plano mestre. Ou seja, se o plano mestre é atualizado a cada 4 anos, o PDZ também deverá ser atualizado a cada 4 anos, com um prazo de submissão de até um ano após a divulgação do novo plano mestre (Portaria nº61, art. 12º).

Outro ponto importante de ser observado é que, se o plano mestre não mencionar diretrizes para a segurança cibernética, muito provavelmente o plano de desenvolvimento e zoneamento também não irá mencionar os processos a serem conduzidos. Isso é uma consequência direta do fato deste segundo documento derivar do primeiro.

Por fim, o Plano Geral de Outorgas (PGO) funciona como um plano de ação. O plano mestre define qual é o *benchmark* a ser alcançado. O PDZ demonstra os processos que precisam ser feitos para que se chegue ao *benchmark.* E o plano geral de outorgas contém todas as pequenas ações práticas que precisam ser realizadas para que ambos os documentos supramencionados sejam cumpridos. Seu conteúdo se concentra nas ações dentro das áreas do porto organizado.

O PGO também é confeccionado e atualizado pelo "poder concedente" e é derivado do PDZ (Portaria nº 61, art. 22), nele são levados em consideração

> [...] o balanço de demanda e capacidade atual e estimada nos portos e terminais existentes e o indicativo de previsão de necessidade de novas instalações portuárias oriundos dos instrumentos de planejamento do Poder Concedente (Portaria nº61, art. 24).

Dito isso, é possível concluir que a Portaria nº61 do Ministério da Infraestrutura se preocupa muito mais com as capacidades físicas dos portos uma vez que seu conteúdo se concentra na regulação dos processos de organização e planejamento de expansão dos portos organizados e suas capacidades.

Cabe ressaltar que as instalações privadas fora da área do porto organizado carecem de mecanismos periódicos que regulem o planejamento da organização física das instalações portuárias.

5.2.2 Lei dos Portos

A Lei 12.815/2013, também conhecida como Lei dos Portos e já mencionada neste relatório anteriormente, é a principal legislação brasileira que regula os portos organizados e a sua exploração, conforme é descrito no art. 1º da mesma.

Já no art. 3º da Lei dos Portos, determina-se que a exploração dos portos organizados e instalações portuárias devem ocorrer de acordo com certas diretrizes. Destas cabe destacar:

> I - Expansão, modernização e otimização da infraestrutura e da superestrutura que integram os portos organizados e instalações portuárias; (...) III - estímulo à modernização e ao aprimoramento da gestão dos portos organizados e instalações portuárias, à valorização e à qualificação da mão de obra portuária e à eficiência das atividades prestadas (LEI DOS PORTOS, 2013).

Como já foi dito no preâmbulo dessa seção do relatório, nenhum dos documentos brasileiros aqui apresentados fazem uma menção direta à segurança cibernética. Entretanto, no trecho da Lei dos Portos supracitado é possível ver uma brecha para a inclusão deste tipo de preocupação no planejamento portuário brasileiro. Ataques cibernéticos são uma consequência direta do avanço da tecnologia e da intensificação do seu uso, questão relativamente nova. Quando a legislação aponta para a modernização, otimização e aprimoramento da gestão e da infraestrutura dos portos, é possível fazer um link com a segurança cibernética. A segurança virtual passou a ser tão relevante quanto a segurança física nos dias de hoje. Afinal, um processo passível de ataques cibernéticos é mais sensível e pode gerar atrasos consideráveis.

O art. 17 da Lei dos Portos, em especial dos incisos VI e XI do §1º, descreve as competências da administração portuária e com isso demonstra uma maior preocupação com a segurança portuária. Nestes incisos, fala-se sobre a responsabilidade da autoridade portuária de fiscalizar as operações, zelando pela segurança e eficiência delas, e reportar a ANTAQ casos de infrações. Mais uma vez, não se fala especificamente sobre a segurança cibernética, mas é interessante perceber como a autoridade portuária tem a responsabilidade de garantir a segurança para o bom funcionamento do porto. Dado o cenário de uso intenso de tecnologia nos processos portuários hoje em dia, urge a necessidade de se prestar uma maior atenção na segurança cibernética.

Por fim, uma última observação a ser feita sobre esta legislação é que, no art. 19, a Lei dos Portos condiciona a exploração de áreas “não afetas às operações portuárias” ao previsto pelo plano de desenvolvimento e zoneamento do porto. Mais uma vez o PDZ é colocado como documento de referência para a gestão portuária e isso reforça a importância de se haver menções à segurança cibernética nele.

Após expor o conteúdo dos três documentos aqui apresentados, vale resumir os objetivos de cada um e os respectivos responsáveis pela elaboração dos arcabouços documentais conforme a Tabela 2:

Tabela 2: Resumo dos Instrumentos Jurídicos do Sistema Portuário Brasileiro

Plano Mestre (PM)	**O que é?**	Instrumento de planejamento de Estado voltado aos complexos portuários que abranjam os portos organizados, considerando as perspectivas do planejamento de transportes em nível estratégico, que visa a direcionar ações e investimentos de curto, médio e longo prazos nos portos, na relação porto-cidade e em seus acessos.
	Responsabilidade?	Ao Poder Concedente caberá a elaboração e atualização dos Planos Mestres dos portos. Entretanto, a Autoridade Portuária deverá participar ativamente da elaboração do respectivo Plano Mestre.
Plano de Desenvolvimento e Zoneamento (PDZ)	**O que é?**	Instrumento de planejamento da Autoridade Portuária, que contempla as estratégias e ações para a expansão e o desenvolvimento integrado, ordenado e sustentável das áreas e instalações do porto organizado.
	Responsabilidade?	Compete à Autoridade Portuária elaborar o PDZ dos portos organizados sob sua gestão e submetê-los à Secretaria Nacional de Portos e Transportes Aquaviários do Ministério de Infraestrutura.
Plano Geral de Outorgas (PGO)	**O que é?**	Instrumento de planejamento de Estado, aderente às diretrizes do planejamento nacional de transportes, aos planos mestres e aos PDZ, com a finalidade de orientar investidores e consolidar projetos de outorga do setor portuário.
	Responsabilidade?	Poder Concedente.

Fonte: Elaboração própria com base na Portaria N° 61 do Ministério da Infraestrutura

Como exposto anteriormente, nenhum dos três documentos apresentados na tabela acima abordam de forma apropriada e aprofundada diretrizes e ações voltadas para a área de segurança cibernética, de forma geral, nem para a área de dados compartilhados do tráfego marítimo, não tendo assim, nada estabelecido de forma clara e diretiva aos portos sobre como as questões de segurança cibernética devem ser tratadas.

Após a elaboração do Plano Mestre, considerando o objetivo aqui já exposto do PDZ de elaborar "as estratégias e ações para a expansão e o desenvolvimento integrado, ordenado e sustentável das áreas e instalações do porto organizado", considera-se fundamental o estabelecimento de regras e parâmetros que deverão nortear a expansão do porto no que tange a segurança cibernética, algo que hoje não é contemplado no PDZ. Sem regras e parâmetros iniciais para a gestão da segurança cibernética, e consequentemente do gerenciamento de dados compartilhados do tráfego marítimo, o crescimento dos portos brasileiros nesta temática será desordenado, assimétrico e não padronizado. Além disso, não foi encontrada nesta pesquisa nenhum fórum portuário que tange a segurança cibernética, onde as autoridades portuárias possam compartilhar ou adquirir boas práticas, algo que precisaria ser motivado pelo próprio Ministério de Infraestrutura. Ainda em relação ao PDZ, o Ministério de Infraestrutura expõe em seu site todos os PDZ dos portos do Brasil, entretanto o ministério não apresenta os documentos equivalentes dos portos privados fora da área do porto organizado, como é o caso do Porto do Açu, porto que faz parte deste relatório.

5.3 Sugestões de Melhoria para os Portos Brasileiros com Base no Caso Europeu

Este relatório buscou ao longo de um ano de pesquisa não só compreender os pontos críticos de segurança cibernética elaborado pela ENISA, como procurou elaborar um formulário no qual foram enviados a todos os portos brasileiros do sudeste listados nas seções anteriores, a fim de compreender como as medidas, políticas e as proposições da ENISA eram trabalhadas nos principais portos do sudeste brasileiro, sendo eles: o Porto de Santos, Rio de Janeiro, Itaguaí, Vitória e Porto do Açu. O formulário foi enviado a todos os portos antepostos. Entretanto, apenas três dos cinco portos responderam. Neste espectro, foram identificadas as principais ameaças e medidas tomadas pelos portos dentro do campo da segurança cibernética, as respostas à pesquisa podem ser encontradas no Anexo I deste relatório.

Apesar de serem portos distintos, foi possível observar que todos os portos respondentes apresentaram na pergunta referente às ameaças mais prováveis de acometerem seus portos, respostas parecidas, sendo a principal "atividades nocivas (como malwares, uso de força bruta,

phishing, roubo de identidade...)". A segunda ameaça mais provável nos portos respondentes é a "falha e mal funcionamento de sistemas, aparelhos e de serviços terceirizados". Em relação às medidas de segurança que o porto já emprega, mesmo não havendo um mecanismo e uma diretriz clara do poder central quanto as diretrizes de segurança, todos os portos respondentes apresentaram as mesmas respostas. Entretanto, essas medidas são originadas de esforços e pesquisas individuais dos portos e não do governo central.

Direcionado a ENISA, apesar de apenas um dos portos respondentes conhecer o relatório da ENISA, foi possível identificar que os portos respondentes já estão alinhados com algumas das sugestões portuárias da ENISA, ou estão em fase de planejamento e implantação. Entretanto, quando se identifica as principais ameaças que podem acometer estes portos, é necessário, de acordo com o conteúdo da ENISA, reforçar as práticas das Políticas Organizacionais e das Medidas Técnicas.

6 CONSIDERAÇÕES FINAIS

Este relatório conclui que atualmente no Estado brasileiro existem diversas lacunas e questões que não estão juridicamente alinhadas quando o assunto é segurança cibernética portuária. A primeira lacuna foi observada na Lei de Portos que, por exemplo, não apresenta a completude das definições dos *stakeholders* pertencentes ao complexo portuário. Consequentemente, por não ter uma robustez conceitual, acaba tendo alguns conceitos incompletos e até mesmo inexistentes, como é possível averiguar na Tabela 1: Localização da Conceituação dos *Stakeholders* Portuários de Nível Federal.

Outro ponto que precisa ser levantado, é que as questões referentes à segurança cibernética portuária deveriam ser estabelecidas por parte do poder central e ser operacionalizado pelas Administrações Portuárias, tendo em vista que pelo fato dos portos serem infraestruturas críticas estarem diretamente ligados ao desempenho econômico do país, são espaços sensíveis a ataques das mais variadas naturezas, inclusive cibernética. Dessa forma, o governo federal precisaria estabelecer políticas, regras e diretrizes a serem seguidas por todas as administrações portuárias presentes no território brasileiro. Entretanto, dando espaço para cada administração portuária estabelecer ações e medidas adicionais de acordo com suas particularidades e necessidades, de forma a acrescentar o arcabouço já estabelecido pelo poder central.

Observou-se, também, a lacuna de documentos equivalentes ao Plano Mestre e PDZ para os portos privados fora da área do porto organizado com a mesma transparência dos Portos públicos.

Dessa forma, entende-se que é necessário que o poder público passe a enxergar a temática da segurança cibernética nos portos brasileiros na hora de elaborar arcabouços documentais, como é o caso do Plano Mestre, mas também é necessário que o legislativo passe a elaborar leis mais robustas e até menos confusas no que concerne a conceitos e nomenclaturas, pois atualmente estes gargalos jurídicos e documentais impactam na segurança cibernética portuária e consequentemente no gerenciamento dos dados de tráfego marítimos.

REFERÊNCIAS BIBLIOGRÁFICAS

AUTORIDADE PORTUÁRIA DO RIO DE JANEIRO (Rio De Janeiro). **Quem Somos**. S.A. Disponível em: https://www.portosrio.gov.br/index.php/pt-br/institucional/quem-somos. Acesso em: 10 nov. 2022.

ANTAQ, Agência Nacional de Transportes Aquaviários. Disponível em: <http://www.portosdobrasil.gov.br>. Acesso em: 21 ago. 2022.

ANTAQ, Agência Nacional de Transportes Aquaviários. **Resolução Normativa nº 07**. Disponível em: https://juris.antaq.gov.br/index.php/2016/06/02/resolucao-normativa-no-07-2016/. Acesso em: 15 de junho de 2022

AZEVEDO. **Lei n. 4.595/64**. S.A. Disponível em: http://www.pge.sp.gov.br/centrodeestudos/revistaspge/revista4/parte1c.htm. Acesso em: 09 set. 2022.

BRASIL. **Lei Nº 9.537, de 11 de dezembro de 1997.** Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9537.HTM. Acesso em: 04 out. 2022.

BRASIL. **Lei Nº 12.815/2013, de 05 de junho de 2013.** Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12815.htm. Acesso em: 04 out. 2022.

BRASIL. Medida Provisória Nº 595 nº 12815, de 05 de junho de 2013.. Brasília: Casa Civil, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12815.htm. Acesso em: 04 out. 2022.

BRASIL. **Departamento de Polícia Federal**. Disponível em: https://www.marinha.mil.br/dpc/sites/www.marinha.mil.br.dpc/files/legislacao/instru-normativa/inst_norm2.pdf. Acesso em: 04 out. 2022.

BRASÍLIA. MINISTÉRIO DE INFRAESTRUTURA. **Poligonais - Portos**. 2017. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/transporte_aquaviario-

antigo/poligonais/poligonais#:~:text=%22Porto%20organizado%22%20%C3%A9%20o%20conjunto,comp%C3%B5em%20o%20%22porto%20organizado%E2%80%9D.. Acesso em: 04 out. 2022.

BRASÍLIA. Receita Federal. Ministério da Fazenda. **Operador Portuário**. S.A. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/subportais-aduana-e-comercio-exterior/intervenientes/habilitacao-em-sistemas-aduaneiros/operador-portuario#:~:text=Operador%20Portu%C3%A1rio%20%C3%A9%20a%20pessoa,da%20%C3%A1rea%20do%20porto%20organizado.. Acesso em: 02 out. 2022.

BRITTO, Paulo Augusto P. de; LUCAS, Vander Mendes; COUTINHO, Paulo César; CARVALHO, Alexandre Xavier Ywata de; OLIVEIRA, André Luís Rossi de; LUSTOSA, Paulo Roberto Barbosa; ALBUQUERQUE, Pedro Henrique Melo; FONSECA, Adelaida Pallavicini. Promoção da concorrência no setor portuário: uma análise a partir dos modelos mundiais e aplicação ao caso brasileiro. **Revista de Administração Pública**, Rio de Janeiro, 2015, v. 49, n. 1, pág. 47 - 72. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/42961. Acesso em: 14 de julho de 2022.

CETESB. **CETESB celebra 53 anos de existência**. 2021. Disponível em: https://cetesb.sp.gov.br/blog/2021/07/24/cetesb-celebra-53-anos-de-existencia/#:~:text=A%20CETESB%20%E2%80%93%20Companhia%20Ambiental%20do,do%20ar%20e%20do%20solo.. Acesso em: 10 set. 2022.

COMPANHIA DE DOCAS DO RIO DE JANEIRO. **Porto do Rio de Janeiro**: história. História. S.A. Disponível em: https://www.portosrio.gov.br/pt-br/portos/porto-do-rio-de-janeiro/historia#:~:text=A%20inaugura%C3%A7%C3%A3o%20oficial%20do%20porto,Brasileira%20de%20Explora%C3%A7%C3%A3o%20de%20Portos.. Acesso em: 10 nov. 2022.

COMPANHIA DE DOCAS DO RIO DE JANEIRO. . **Porto do Rio Século XXI**: desenvolvimento e integração porto-cidade. Desenvolvimento e Integração Porto-Cidade. 2020. Disponível em: COMPANHIA DE DOCAS DO RIO DE JANEIRO. Acesso em: 10 nov. 2022.

COMPANHIA DE DOCAS DO RIO DE JANEIRO (Rio de Janeiro). **Plano de Desenvolvimento e Zoneamento**. 2016. Disponível em: https://www.portosrio.gov.br/sites/default/files/inline-files/pdz_-_2016_do_porto_do_rio_de_janeiro.pdf. Acesso em: 12 dez. 2022.

COMPANHIA DE DOCAS DO RIO DE JANEIRO **PLANO DE DESENVOLVIMENTO E ZONEAMENTO PORTUÁRIO**: porto de Itaguaí. PORTO DE ITAGUAÍ. 2019. Disponível em: https://www.gov.br/infraestrutura/pt-br/centrais-de-conteudo/pdz13-pdf. Acesso em: 13 out. 2022.

ENISA. **Port Cybersecurity: Good practices for cybersecurity in the maritime sector**. União Europeia, 2019. Disponível em: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector. Acesso em: 20 de maio de 2022.

FARRANHA, Ana Claudia; FREZZA, Conrado da Silveira; e BARBOSA, Fabiana de Oliveira. Nova lei dos portos: desafios jurídicos e perspectivas de investimentos. **Revista Direito GV,** São Paulo, 2015, v. 11, n. 1, pág. 89 - 116. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/revdireitogv/article/view/56794. Acesso em: 14 de julho de 2022.

GONÇALVES, Alcindo. **O CONCEITO DE GOVERNANÇA**. 2005. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/XIVCongresso/078.pdf. Acesso em: 10 jun. 2022.

LONDRES. GOVERNO DO REINO UNIDO. **MGN 401 (M+F) Amendment 3 Navigation**: vessel traffic services (VTS) and local port services (LPS) in the UK. Vessel Traffic Services (VTS) and Local Port Services (LPS) in the UK. 2022. Disponível em: https://www.gov.uk/government/publications/mgn-401-mf-amendment-3-navigation-vessel-traffic-services-vts-and-local-port-services-lps-in-the-uk/mgn-401-mf-amendment-3-navigation-vessel-traffic-services-vts-and-local-port-services-lps-in-the-uk#local-port-services-lps. Acesso em: 01 nov. 2022.

MARINHA DO BRASIL. Mapa Sensitivo. S.A. Acesso em: https://www.marinha.mil.br/dpc/node/3503.

MINISTÉRIO DE INFRAESTRUTURA. BRASÍLIA. **Sistema Portuário Nacional**. 2022. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/transporte_aquaviario-antigo/sistema-portuario. Acesso em: 03 ago. 2022.

PORTO DO AÇU. **Regulamento Portuário,** 2ª. Edição, Revisão 01. Disponível em: https://portodoacu.com.br/wp-content/uploads/2022/09/20191219-PdA-Regulamento-Portuario-PORTUGUES-2ed-REV-01.pdf. Acesso em: 17 de novembro de 2022

SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS. **Agentes que atuam no Porto**. S.A. Disponível em: https://www.portodesantos.com.br/conheca-o-porto/agentes-que-atuam-no-porto/. Acesso em: 21 jul. 2022.

SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS. **Plano Estratégico 2021-2025**. Disponível em: https://www.portodesantos.com.br/wp-content/uploads/Plano-Estrategico-2021-2025.pdf. Acesso em 04 de dezembro de 2022.

SANTOS. AUTORIDADE PORTUÁRIA DE SANTOS. **Manual SGPI - análise e avaliação de riscos de segurança da informação e privacidade**. Disponível em: https://intranet.portodesantos.com.br/docs_codesp/doc_codesp_pdf_site.asp?id=139250. Acesso em 05 de dezembro de 2022.

SOUSA, Erivelto Fioresi de. **EFICIÊNCIA E GOVERNANÇA PORTUÁRIA**: evidência do sistema portuário brasileiro. EVIDÊNCIA DO SISTEMA PORTUÁRIO BRASILEIRO. 2019. Disponível em: https://producaoonline.org.br/rpo/article/download/3037/1812. Acesso em: 20 ago. 2022.

TOMAZETTE, Marlon. **Empresário**. 2018. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/231/edicao-

1/empresario#:~:text=A%20empresa%20%C3%A9%20uma%20atividade,no%20mesmo%20sentido%20do%20art.. Acesso em: 20 jun. 2022.

UNCTAD. **Review of Maritime Transport.** 2021. Disponível em: https://unctad.org/publication/review-maritime-transport-2021. Acesso em: 03 de março de 2022

VIEIRA, Sérgio. **GOVERNANÇA CORPORATIVA E CONSELHEIRO EMPRESARIAL**. S.A. Disponível em: https://www.sergiovieira.com.br/governanca-corporativa#:~:text=Juiz%20Arbitral,controle%20e%20demais%20partes%20interessadas.. Acesso em: 10 jun. 2022.

VIEIRA, João; FIALHO, Gilberto Olympio Mota. MODERNIZAÇÃO DA GESTÃO PORTUÁRIA E PLANEJAMENTO OPERACIONAL INTEGRADO. **Revista Eletrônica de Estratégia & Negócios**, [S.L.], v. 13, n. 0, p. 196, 24 jun. 2020. Universidade do Sul de Santa Catarina - UNISUL. http://dx.doi.org/10.19177/reen.v13e0i2020196-224. Disponível em: https://portaldeperiodicos.animaeducacao.com.br/index.php/EeN/article/download/9311/pdf/23434#:~:text=A%20governan%C3%A7a%20portu%C3%A1ria%20pode%20ser,consequentemente%20a%20competitividade%20do%20porto.. Acesso em: 10 jun. 2022.

VILLAS BOAS, Marcelo Santiago; BRIGLIA, Tatiana; VIDAL, Nathalia. **IMPLEMENTAÇÃO DO SISTEMA DE INFORMAÇÃO E GERENCIAMENTO DO TRÁFEGO DE EMBARCAÇÕES**: VTMIS no estado do rio de janeiro. VTMIS NO ESTADO DO RIO DE JANEIRO. 2021. Disponível em: https://cidesport.com/wp-content/uploads/2021/10/Anais_CIDESPORT.pdf. Acesso em: 10 out. 2022.

VILLAS-BÔAS, 2020 *apud* **Relatório de pesquisa Compartilhamento e Integração de Informações do Movimento Marítimo**, p. 36. Disponível em: https://www.marinha.mil.br/ppgem/sites/www.marinha.mil.br.ppgem/files/upload/relatorio_egn-ezute_ciclo_de_pesquisa_2020-2021_compartilhamento_e_integracao_de_informacoes_-_cluster.pdf. Acesso em: 10 de outubro de 2022

ANEXO I: Perguntas e Respostas do Formulário sobre Segurança Cibernética

Perguntas	Respostas
Com base na realidade do porto em que você está inserido e levando em conta a segurança do espaço físico do porto e de seu conteúdo, quais são os principais desafios oriundos da gestão dos dados de tráfego marítimo compartilhados?	1- Resiliência a cyber ataques e manutenção do serviço plenamente operacional 24h/7d; 2- Manter o nível de conscientização de segurança da informação dos colaboradores elevado.
Com base na realidade do porto em que você está inserido e levando em conta a segurança cibernética das tecnologias de informação, quais são os principais desafios oriundos da gestão dos dados de tráfego marítimo compartilhados?	1- Duplicidade de provedores de internet e firewall apto a proteger de ataques de hackers; 2- Manter o nível de conscientização de segurança da informação dos colaboradores elevado.
Esta pesquisa tem como base o manual de boas práticas para a segurança cibernética nos portos, emitido pela Agência para Segurança Cibernética da União Europeia (ENISA, na sigla em inglês) em novembro de 2019. Você já tinha conhecimento sobre esta publicação?	1- Não; 2- Sim; 3- Não.
Dada a lista de possíveis ameaças abaixo, quais você listaria como sendo as mais prováveis de acometerem o porto ao qual está ligado?	1- Atividades nocivas (como malwares, uso de força bruta, phishing, roubo de identidade...), Desastres ambientais e naturais, Suspensão de internet, de subsídios, de mão de obra e/ou de apoio, falha e mal funcionamento de sistemas, aparelhos e de serviços terceirizados; 2 - Atividades nocivas (como malwares, uso de força bruta, phishing, roubo de identidade...); 3- Falha e mal funcionamento de sistemas, aparelhos e de serviços terceirizados.
Dadas as medidas de segurança listadas abaixo, quais já são empregadas no porto ao qual está ligado?	1- Políticas organizacionais (existência de definição de políticas e governança em matéria de tecnologias da informação (TI) e tecnologias operacionais (TO), aplicação de melhores práticas de cibersegurança, especialmente para a maioria dos bens críticos, com uma abordagem baseada no risco)., Práticas organizacionais (existência de definição de práticas e processos relevantes relativos à gestão de Tecnologia da Informação e Tecnologia Operacional, a serem seguido por todos os funcionários do porto ou mais especificamente pelas equipes de TI e TO em suas operações diárias dentro do ecossistema portuário)., Medidas técnicas (existência e aplicação de várias medidas técnicas, a fim de evitar ciberataques nos portos de Tecnologia da Informação ou Tecnologias Operacionais, detecção e reagir a qualquer ataque e ser resiliente em caso de um grande impacto de um ciberataque); 2- Políticas organizacionais (existência de definição de políticas e governança em matéria de tecnologias da informação (TI) e tecnologias operacionais (TO), aplicação de melhores práticas de cibersegurança, especialmente para

Perguntas	Respostas
	a maioria dos bens críticos, com uma abordagem baseada no risco)., Práticas organizacionais (existência de definição de práticas e processos relevantes relativos à gestão de Tecnologia da Informação e Tecnologia Operacional, a serem seguido por todos os funcionários do porto ou mais especificamente pelas equipes de TI e TO em suas operações diárias dentro do ecossistema portuário)., Medidas técnicas (existência e aplicação de várias medidas técnicas, a fim de evitar ciberataques nos portos de Tecnologia da Informação ou Tecnologias Operacionais, detecção e reagir a qualquer ataque e ser resiliente em caso de um grande impacto de um ciberataque). 3- Políticas organizacionais (existência de definição de políticas e governança em matéria de tecnologias da informação (TI) e tecnologias operacionais (TO), aplicação de melhores práticas de cibersegurança, especialmente para a maioria dos bens críticos, com uma abordagem baseada no risco)., Práticas organizacionais (existência de definição de práticas e processos relevantes relativos à gestão de Tecnologia da Informação e Tecnologia Operacional, a serem seguido por todos os funcionários do porto ou mais especificamente pelas equipes de TI e TO em suas operações diárias dentro do ecossistema portuário)., Medidas técnicas (existência e aplicação de várias medidas técnicas, a fim de evitar ciberataques nos portos de Tecnologia da Informação ou Tecnologias Operacionais, detecção e reagir a qualquer ataque e ser resiliente em caso de um grande impacto de um ciberataque).
Dentre os sistemas listados no quadro abaixo, quais são utilizados pelo porto em que atua?	1- Port Community System (PCS), VTS / VTMIS; 2- Port Community System (PCS); 3- Port Corporate Systems, VTS / VTMIS, Sistema de Gerenciamento do Porto (SGP) (proprietário do Porto).
Dada as tecnologias e redes de comunicação listadas abaixo, quais são utilizadas pelo porto em que atua?	1- Rádio, Protocolos, Servidores, Redes de comunicação, Hubs, roteadores e comutadores, Redes de segurança, Nuvem; 2- Rádio, Protocolos, Servidores, Redes de comunicação, Hubs, roteadores e comutadores, Redes de segurança, Nuvem; 3- Rádio, Protocolos, Servidores, Redes de comunicação, Hubs, roteadores e comutadores, Redes de segurança.

Perguntas	Respostas
Poderia explicar mais a fundo quais medidas de segurança são utilizadas no porto ao qual faz parte?	1- Estabelecimento de um sistema de gestão de segurança da informação. Implantação do ISPS-CODE. Adoção de uma política de segurança da informação rigorosa; 2- São utilizadas as medidas tradicionais e consagradas aplicadas no ambiente empresarial/corporativo.
Há alguma medida de segurança cibernética a qual o porto que faz parte pretende implementar ou está em processo de implementação?	1- Uso de antivírus atualizado continuamente, bloqueio de tela, impedimento de instalação de SW externos e segregação da rede local de Docas; 2- Obtenção da ISO 27001; 3- Informação não disponibilizada pela área de tecnologia de informação do Porto.