Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Victoria Paschoalin Morales

Wesley Camargo Moreira

RANSOMWARE EM INFRAESTRUTURAS MARÍTIMAS:

Lições do Ataque à Maersk para a Frota Marítima Brasileira.

Americana, SP

2025

Victoria Paschoalin Morales
Wesley Camargo Moreira

RANSOMWARE EM INFRAESTRUTURAS MARÍTIMAS.

Lições do Ataque à Maersk para a Frota Marítima Brasileira.

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança da Informação.

Orientador: Prof. Me. Rafael Rodrigo Martinati

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Victoria Paschoalin Morales e Wesley Camargo Moreira e orientado pelo Prof. Me. Rafael Rodrigo Martinati.

Americana, SP
2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

MORALES, Victoria Paschoalin

Ransomware em infraestruturas marítimas: Lições do ataque à Maersk para a frota marítima brasileira.. / Victoria Paschoalin Morales, Wesley Camargo Moreira – Americana, 2025.

48f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Rafael Rodrigo Martinati

1. Segurança em sistemas de informação. I. MORALES, Victoria Paschoalin, II. MOREIRA, Wesley Camargo III. MARTINATI, Rafael Rodrigo IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Vitória Paschoalin Morales

Wesley Camargo Moreira

RAMSOMWARE EM INFRAESTRUTURAS MARÍTIMAS: lições do ataque à Maersk para frota marítima brasileira

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 08 de novembro de 2025.

Banca Examinadora:

Rafael Rodrigo Martinati
Mestre
Fatec Americana "Ministro Ralph Biasi"

Rodrigo Brito Battilana
Mestre
Fatec Americana "Ministro Ralph Biasi"

Rogério Nunes de Freitas
Mestre
Fatec Americana "Ministro Ralph Biasi"

AGRADECIMENTOS

Em primeiro lugar, gostaríamos de agradecer aos nossos pais pelo incentivo e carinho.

Ao nosso orientador, Rafael Rodrigo Martinati, pela dedicação, pelas correções e pelo incentivo durante o desenvolvimento do trabalho.

À professora Maria Cristina Aranda, pelas correções e sugestões para o aprimoramento do trabalho.

E aos demais que contribuíram de alguma forma na realização deste projeto.

RESUMO

Este trabalho analisa os impactos do *ransomware* em infraestruturas críticas do setor marítimo, com foco no ataque NotPetya à A.P. Moller-Maersk em 2017, e discute suas implicações para a frota marítima brasileira. A pesquisa, que é de caráter qualitativo, exploratório e descritivo, foi conduzida por meio de revisão bibliográfica, pesquisa documental e estudo de caso. O referencial teórico aborda os pilares da Segurança da Informação, os principais tipos de *malware*, a evolução do *ransomware* e as vulnerabilidades resultantes da convergência entre Tecnologia da Informação (TI) e Tecnologia Operacional (TO) em ambientes navais. O estudo de caso detalha a infecção, propagação e consequências do NotPetya, destacando falhas de governança e ausência de segmentação de redes que ampliaram os impactos globais do ataque. Com base nas lições aprendidas, foram propostas recomendações aplicáveis ao contexto brasileiro, incluindo segmentação lógica com VLANs, implementação de *firewalls*, adoção de políticas de *backup offline* e fortalecimento da governança de TI por meio da Gestão de Riscos Integrada e de planos de resposta a incidentes. Conclui-se que a mitigação de riscos no setor marítimo nacional depende menos da adoção de novas tecnologias e mais da aplicação consistente de boas práticas de arquitetura de redes e de governança cibernética, alinhadas a normas internacionais e à Estratégia Nacional de Segurança Cibernética.

Palavras-Chave: *Ransomware*; infraestruturas críticas; cibersegurança marítima.

ABSTRACT

This study analyzes the impact of ransomware on critical maritime infrastructures, focusing on the 2017 NotPetya attack against A.P. Moller-Maersk, and discusses its implications for the Brazilian maritime fleet. The research, which is qualitative, exploratory, and descriptive in nature, was conducted through bibliographic review, documentary research, and a case study. The theoretical framework addresses the pillars of Information Security, the main types of malware, the evolution of ransomware, and the vulnerabilities resulting from the convergence of Information Technology (IT) and Operational Technology (OT) in naval environments. The case study details the infection, propagation, and consequences of NotPetya, highlighting governance failures and the absence of network segmentation that amplified the global impact of the attack. Based on the lessons learned, recommendations applicable to the Brazilian context were proposed, including logical segmentation with VLANs, implementation of firewalls, adoption of offline backup policies, and strengthening IT governance through Integrated Risk Management and incident response plans. It is concluded that risk mitigation in the national maritime sector depends less on adopting new technologies and more on consistently applying best practices in network architecture and cyber governance, aligned with international standards and the Brazilian National Cybersecurity Strategy.

Keywords: *Ransomware; critical infrastructures; maritime cybersecurity.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AIS	Sistema de Identificação Automática
AMB	Autoridade Marítima Brasileira
ANCiber	Agência Nacional de Cibersegurança
APF	Administração Pública Federal
BIMCO	*Baltic and International Maritime Council*
CID	Confidencialidade, Integridade e Disponibilidade
CNCiber	Comitê Nacional de Cibersegurança
DPC	Diretoria de Portos de Costas
ECDIS	Sistema de Informação e Visualização de Cartas Eletrônicas
E-Ciber	Estratégia Nacional de Cibersegurança
GNL	Gás Natural Liquefeito
GPS	Sistema de Posicionamento Global
GRI	Gestão de Riscos Integrada
GSI	Gabinete de Segurança da Presidência da República
IBL	Instituto Brasileiro de Logística
IC	Infraestrutura Crítica
ICM	Infraestrutura Crítica Marítima
ICS	Sistema de Controle Indústrial
IMO	Organização Marítima Internacional
IP	*Internet Protocol*
ISM	Código Internacional de Gestão de Segurança
MBR	Registro Mestre de Inicialização
MSC	Comite de Segurança Marítima
NIST	Instituto Nacional de Padrões e Tecnologia

NORMAM	Normas da Autoridade Marítima
NSA	Agência de Segurança Nacional
PMN	Política Marítima Nacional
PNCiber	Política Nacional de Cibersegurança
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança e Infraestruturas Críticas
PRI	Plano de Resposta a Incidentes
RaaS	*Ransomware as a Service*
ReGIC	Rede Federal de Gestão de Incidentes Cibernéticos
RUSI	Royal United Services Institute
SATCOM	Comunicação via Satélite
SGS	Sistema de Gerenciamento de Segurança
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TME	The Maritime Executive
TO	Tecnologia Operacional
VLAN	*Virtual Local Area Network*

SUMÁRIO

1. INTRODUÇÃO

A relevância do setor marítimo para o comércio global é evidente, estima-se que 90% das mercadorias são transportadas por vias marítimas, o que demonstra a relevância dessa infraestrutura para o abastecimento das nações e a manutenção das cadeias de suprimentos mundiais (International Maritime Organization, 2017). Nesse contexto, o Brasil não se destaca apenas pela extensão de sua costa, mas também pela sua profunda dependência do setor, por onde tramita cerca de 71% das suas exportações. (Organização para a Cooperação e Desenvolvimento Econômico, 2022). Entretanto, essa mesma dependência o converte em um alvo estratégico e evidencia a sua vulnerabilidade a ameaças cibernéticas.

A crescente digitalização do setor, impulsionada pela convergência entre Tecnologia da Informação (TI) e Tecnologia Operacional (TO), embora tenha ampliado a sua eficiência, expõe os sistemas marítimos de forma simultânea a riscos cada vez mais sofisticados. Dentre esses riscos, os ataques de *ransomware* têm crescido e se destacado pela sua dupla capacidade de comprometer dados críticos e paralisar operações vitais. Essa tendência é corroborada por um relatório de 2020 do The Maritime Executive (TME), que revelou um aumento de 400% em ciberataques, com ênfase significativa em *malwares*, *ransomware* e *phishing*. A gravidade desses incidentes é destacada pela Fortinet (2024), que os classifica entre os mais graves para a segurança cibernética, levando em conta que ele criptografa os dados e demanda um pagamento para a liberação.

O potencial destrutivo desses ataques não é algo hipotético. O incidente envolvendo a A.P. Moller-Maersk em 2017 exemplifica de forma clara como falhas de governança e a ausência de segmentação de redes podem culminar em danos de grande escala. De acordo com Mathews (2017), o ataque NotPetya paralisou operações em escala global, gerando prejuízos estimados entre 200 e 300 milhões de dólares. Esse caso não se limitou apenas as fragilidades técnicas, mas também expôs as defasagens organizacionais no enfrentamento de incidentes cibernéticos.

Diante desse cenário, torna-se necessário compreender os riscos que afetam a infraestrutura marítima nacional e identificar práticas que possam ser adaptadas ao contexto brasileiro. Como observa Oliveira (2022), a vulnerabilidade das infraestruturas críticas marítimas brasileiras ocorre não apenas pela carência de investimentos tecnológicos, mas também pela ausência de uma governança integrada de riscos cibernéticos.

Assim, este trabalho define a seguinte pergunta de pesquisa: Quais medidas de segurança cibernética podem ser aplicadas à frota marítima brasileira a partir das lições aprendidas com o ataque NotPetya à empresa Maersk?

Para responder a essa questão, o estudo estabelece como objetivo geral, analisar o ataque de *ransomware* sofrido pela Maersk, identificando suas causas e consequências, a fim de propor medidas de segurança cibernética aplicáveis à frota marítima brasileira. E como objetivos específicos:

- Contextualizar os conceitos fundamentais de Segurança da Informação, *malware* e *ransomware*, bem como a convergência entre TI e TO no setor marítimo;
- Descrever e analisar o ataque NotPetya à Maersk, destacando suas falhas de segurança e impactos organizacionais;
- Identificar vulnerabilidades da frota marítima brasileira em relação a incidentes cibernéticos;
- Propor recomendações técnicas e de governança voltadas à proteção cibernética das infraestruturas marítimas nacionais.

O trabalho está estruturado da seguinte forma: no Capítulo 2, apresenta-se o referencial teórico, abordando os principais conceitos relacionados à Segurança da Informação e as ameaças digitais. O Capítulo 3 descreve a metodologia utilizada, caracterizada como qualitativa, exploratória e descritiva. O Capítulo 4 detalha o estudo de caso da Maersk, enquanto o Capítulo 5 propõe recomendações aplicáveis ao Brasil. Por fim, o Capítulo 6 apresenta as considerações finais, retomando a questão-problema e apontando sugestões para pesquisas futuras.

2. REFERENCIAL TEÓRICO

Este capítulo fundamenta a base teórica necessária para a análise do ataque de *ransomware* NotPetya à infraestrutura da A.P. Moller-Maersk. Para isso, inicialmente são abordados os principais conceitos que compõem o escopo da pesquisa, com a definição dos pilares da Segurança da Informação e a sua aplicação. Por fim, a discussão se aprofunda nas vulnerabilidades e na superfície de ataque de embarcações marítimas.

2.1 SEGURANÇA DA INFORMAÇÃO

O campo que visa garantir a proteção dos dados em todos os níveis de uma organização, e que abrange os aspectos tecnológicos, organizacionais e humanos é a Segurança da Informação. Segundo Laudon e Laudon (2010), “a informação é um dos ativos mais importantes de uma organização, sendo essencial para a tomada de decisões e para a vantagem competitiva”.

A tríade Confidencialidade, Integridade e Disponibilidade (CID) é o principal modelo nessa área, e nele se estabelece, de forma respectiva, que as informações devem ser acessadas somente por pessoas autorizadas, que não sejam modificadas de forma indevida e que estejam disponíveis quando necessário. Além dessa tríade, outros princípios são citados frequentemente, como autenticidade, responsabilidade e não repúdio, principalmente em ambientes marítimos.

2.1.1 Os Princípios da Segurança da Informação.

De acordo com o projeto de norma ISO/IEC 27002:2022, a Segurança da Informação se fundamenta em três pilares fundamentais: Confidencialidade, Integridade e Disponibilidade. Eles formam a base para a elaboração de políticas e controles de segurança em qualquer organização.

- **Confidencialidade**: Esse princípio está relacionado à política de acesso, no qual se estabelece quais dados um determinado usuário ou grupo de usuários podem acessar, conforme as suas funções e responsabilidades em uma organização. Também se refere aos dados disponíveis para acesso público, geralmente destinado a pessoas externas. Levando isso em conta, caso um agente não autorizado obtenha uma senha de acesso a dados privados, isso será considerado uma violação da confidencialidade.

- **Integridade:** É o princípio relacionado à confiabilidade dos dados, ou seja, ele trata de alterações, adições ou exclusões não autorizadas no banco de dados de uma empresa.

- **Disponibilidade:** Princípio relacionado a garantia de acesso autorizado. Consiste majoritariamente em manter a robustez de hardware e software, a fim de impedir que os sites e servidores da organização fiquem inativos.

Esses princípios são corroborados por mecanismos, políticas e cultura. Enquanto os mecanismos podem ser implementados através de hardware e software, as políticas são fundamentadas em regras e normas, já a cultura é referente ao conhecimento que as pessoas envolvidas na organização possuem.

2.1.2 *Softwares* Maliciosos (*Malware*): Definição e classificações

O termo *malware*, que é uma contração de *malicious software* (*software* malicioso), se refere a qualquer programa ou código intrusivo desenvolvidos por cibercriminosos com o intuito de danificar, explorar ou obter acesso não autorizado a sistemas digitais (Kaspersky, 2024). Na tabela a seguir, são apresentadas as principais categorias de *malware*.

Tabela 1: Tipos de *malware*

Tipo de *malware*	**Característica principal**
Vírus	Possui a capacidade de autorreplicação, ou seja, realiza cópias de si mesmo ou infecta arquivos ou programas já existentes no computador. Necessita de interação manual para ser ativado.
Worm	Similar ao vírus, porém atua de forma automática, sem a necessidade de interação com o usuário para ativação. Geralmente estão anexados em *e-mails*.
Backdoor	Ataques desse tipo exploram as vulnerabilidades presentes em um sistema ou programa. Pode ser intencional, isto é, criado de maneira proposital por desenvolvedores para ignorar algumas defesas e facilitar a experiência dos usuários.
Spyware	O seu principal objetivo é a violação da privacidade, não tem o intuito proposital de danificar o dispositivo. Atua na coleta de informações de um computador de um usuário e enviando-as a terceiros.
Adware	Utiliza anúncios e *pop-ups* indesejados, que podem ser utilizados para distribuição de outros tipos de *malware*, como *spyware e* vírus.
Botnet	Se trata de um conjunto de dispositivos infectados que seguem instruções dadas por um atacante. Podem ser criados através de câmeras IP, roteadores e celulares Android.
Trojan (Cavalo de Troia)	Programa que esconde uma aplicação maliciosa e cria *backdoors* para que invasores explorem essas falhas e causem danos.
Ransomware	Criptografa os arquivos da vítima ou bloqueia o acesso ao sistema, após isso, exige o pagamento de um resgate para recuperação dos dados.

Fonte: Autoria própria, baseada em Grasso (2024)

2.1.3 *Ransomware*

O *ransomware* é um tipo de *malware* que impossibilita o acesso a dados ou sistemas, e demanda o pagamento de um resgaste para reestabelecer o acesso (Fortinet, 2024). Ele se transformou em uma das ameaças cibernéticas mais lucrativas e destrutivas, e isso é visível no seu impacto em organizações de todos os portes e setores.

O modus operandi de um *ransomware* pode se resumir a três etapas consecutivas, a infecção, a criptografia e por último a extorsão (Grasso, 2024). Na etapa inicial, o *ransomware* se infiltra no sistema por meio de *e-mails* de *phishing*, *downloads* de *sites* suspeitos, ou até mesmo através de vulnerabilidades de *software* não corrigidas. Em seguida, o *ransomware* criptografa os arquivos da vítima, fazendo com que fiquem ilegíveis. Algumas variações mais robustas podem até criptografar redes inteiras e arquivos de *backup*. Na etapa final, ele exibe uma solicitação de resgate, no qual a vítima é informada sobre o ataque e posteriormente exigindo um pagamento, geralmente em criptomoedas como o Bitcoin, para obter a chave de descriptografia. Há também outras variantes, conhecidas como *leakware* ou *doxware*, que ameaçam publicar os dados roubados publicamente caso o resgate não seja pago. Na visão da vítima, o principal objetivo ao realizar esse pagamento, consiste em obter acesso à chave de descriptografia e em seguida recuperar o acesso aos dados.

A primeira menção de *ransomware* ocorreu em 1989, com o AIDS Trojan, que utilizava criptografia simétrica e era distribuída por meio de disquetes. Segundo Grasso (2024), mesmo com essa data de criação, a sofisticação surgiu apenas em meados de 2005, com o novo alvo sendo organizações ao invés de indivíduos. O *ransomware-as-a-service* (RaaS) é considerado uma evolução no método de negócios do *ransomware*, nele grupos de criminosos desenvolvem o *malware* e o licenciam para afiliados, que executam os ataques e dividem os lucros. Essa modalidade reduziu de forma significativa os obstáculos de entrada para cibercriminosos, além de impulsionar a propagação de ataques.

Segundo Horduna *et al.* (2022), existem cinco tipos principais de *ransomware*, cada um com características específicas, conforme apresentado na tabela 2:

Tabela 2: Tipos de *ransomware*

Nome	**Característica**
Locker	Bloqueia o acesso aos recursos computacionais, permitindo apenas a interação com o sistema de pagamento.
Crypto-ransomware	Criptografa os dados da vítima, exigindo um resgate para a chave de descriptografia.
Leakware	Ameaça divulgar os dados confidenciais, afetando a imagem pública de empresas, sem destruir ou bloquear acesso aos dados.
Scareware	Utiliza engenharia social para assustar o usuário através de mensagens *pop-up* falsas, induzindo-o a instalar outro *malware*.
Ransomware-as-a-Service (RaaS)	Através de um esquema de afiliados, pessoas - com baixo conhecimento técnico - podem espalhar o *ransomware* e receber porcentagem do resgate.

Fonte: Autoria própria, baseada em Horduna et al (2022).

Um método amplamente utilizado para a disseminação do *ransomware* é a engenharia social, trata-se de manipulação psicológica empregada para persuadir a vítima, a sua propagação utiliza *phishing,* Tupinambá (2020, p. 15 *apud* Coelho Júnior; Silva, 2024, p. 26) compreende-o como:

> [...] uma simulação, na qual a vítima é enganada para que, pensando em tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégio.

Essa é uma das formas mais comuns para a propagação do *ransomware*. Entre outros métodos citados por Horduna *et al.* (2022), pode-se mencionar a capacidade de auto propagação, *botnets*, *malvertising* e *cross-site scripting.* No caso do NotPetya, o estudo de caso selecionado, a capacidade de auto propagação foi o vetor principal que permitiu a disseminação em larga escala, o tema será introduzido no tópico a seguir.

2.2 VULNERABILIDADES EM SISTEMAS NAVAIS

Segundo Freire (2022) a digitalização converteu os navios modernos em complexos sistemas ciber-físicos, nos quais a TI e a TO se integram. Porém, se por um lado essa união otimiza as operações, por outro, aumenta de forma significativa a superfície de ataque, expondo sistemas críticos de navegação. Nessa seção, o foco se move da ameaça para a superfície de ataque, detalhando as suas vulnerabilidades e interconexão.

A análise do ataque NotPetya demonstra que a sua eficácia não se deve apenas à técnica do *malware*, mas também à existência de vulnerabilidades no ambiente comprometido. O setor marítimo, em sua crescente digitalização, deixou todos os objetos ligados à área em um complexo sistema ciber-físico, nas quais a TI e as TO estão cada vez mais interligadas.

2.2.1 A Convergência TI/TO no Ambiente Marítimo

A convergência TI/TO se refere à integração de sistemas de TI, geralmente focados em dados e comunicação (p. ex., *e-mail*, sistemas de gerenciamento), com sistemas de TO, que monitoram e controlam processos físicos (p. ex., motores, sistemas de navegação). No ambiente marítimo, essa convergência permite o monitoramento remoto e a otimização de rotas e consumo de combustível, mas também cria um ponto de entrada para ameaças cibernéticas (Cassell, 2024). O autor alega ainda:

> A convergência TI/TO faz com que as fronteiras entre as funções de rede de TI e as funções de controle crítico de TO se tornem difusas, apresentando um desafio para os operadores entenderem completamente como os sistemas interagem entre si.

Essa informação é aprofundada no relatório da RUSI, de acordo com Polemi e Maele (2023), a natureza do setor marítimo, que mescla ativos físicos e cibernéticos, expõe o ecossistema marítimos a ameaças híbridas.

No aspecto físico, pode-se mencionar os veículos de carga/descarga, distribuição e armazenamento de Gás Natural Liquefeito (GNL), que são executados por sistemas físicos, mecânicos autônomos e semi-autônomos e maquinário, dentre

alguns destes, pode-se mencionar: navios, caminhões, guindastes, portões e vedações eletrônicas.

Já no aspecto cibernético ou digital, se destacam os sistemas de *software* logísticos, um exemplo disso são os sistemas ciber-físico industriais, como SCADA e sistemas de vigilância, que são utilizados para auxiliar diretamente nas operações físicas. Tendo isso em vista, enquanto os sistemas de TO controlam as operações físicas, que são executadas por máquinas, os sistemas de TI atuam na gestão de dados e informação.

Em adição a isso, Loureiro (2016) aponta que o principal motor no aumento da exposição a riscos de incidentes e ataques cibernéticas, está intrinsecamente ligado à crescente dependência de sistemas e serviços conectados a uma rede. Embora essa conectividade tenha trazido benefícios explícitos, como o aumento da velocidade para atividades essenciais, também trouxe uma ampliação na superfície de ataque.

Levando isso em conta, a crescente interdependência entre o mundo físico e cibernético no ambiente marítimo torna imprescindível analisar de forma detalhada os sistemas operacionais mais críticos a bordo, como os de navegação, automação e comunicação, que são alvos visados de forma primária em ciberataques.

No capítulo seguinte, serão abordados os principais sistemas críticos de bordo, como o ECDIS (Navegação), o AIS (Automação) e o SATCOM (Comunicação via Satélite), além de analisar as suas principais vulnerabilidades.

2.2.2 Sistemas Críticos de Bordo

Diversos sistemas a bordo são essenciais para a segurança e operação de um navio. Polemi e Maele (2023) destacam que diversas tecnologias são utilizadas em navios. Dentre elas, destacam-se os Sistemas de Posicionamento, o Sistema de Informação e Visualização de Cartas Eletrônicas (ECDIS), o Sistema de Controle Industrial (ICS), o Sistema de Identificação Automática (AIS), entre outros.

O sistema ICS fornece automação integrada, além de controlar e monitorar vários subsistemas da embarcação, como propulsão, geração de energia e controle de carga. Ataques direcionados a ele podem causar a perda de controle do motor, blecautes ou manipulação de cargas perigosas. Há também o AIS, um sistema utilizado para monitoramento de curto alcance em navios e Serviços de Tráfego de

Embarcações. Bartlett (2015, *apud* Loureiro, 2016) aponta que através de testes realizados no sistema AIS, foi comprovada a possibilidade de fazer com que navios desaparecessem dos sistemas de rastreamento e de embarcações não existentes serem exibidas neles, além de emitir alertas falsos de socorro, colisão ou até mesmo alterar informações sobre o curso dos navios.

O principal elo de um navio com o mundo exterior são as telecomunicações via satélite, que desempenham um papel fundamental, ao prover acesso à internet e comunicação de voz. Entre as principais ameaças dessa área, pode-se destacar: a intercepção de dados (*eavesdropping*), onde a falta de criptografia adequada permite a intercepção da comunicação, o uso de *jamming* e *spoofing* de sinais, utilizados pelos invasores para bloqueio (*jamming*) e falsificação (*spoofing*) dos sinais de satélite, visando interromper a comunicação, além de enganar os sistemas de navegação, e consequentemente, comprometer os terminais, nos quais terminais de usuários a bordo podem ser alvos de ataques que visam obter acesso à rede interna do navio.

Por último, o ECDIS também é considerado como infraestrutura crítica. Entre as suas vulnerabilidades, pode-se mencionar os sistemas operacionais desatualizados, tendo em vista que vários sistemas ECDIS funcionam em versões antigas do Windows (p. ex., XP), que possuem vulnerabilidades conhecidas, devido a não receberem mais atualizações de segurança. Outra fragilidade notável são as conexões inseguras, ou seja, a conexão com outros sistemas, como GPS e radar, que também podem ser utilizadas como vetor de ataque se não for protegido de forma adequada. Há também a manipulação de dados, no qual um invasor pode modificar as cartas náuticas, levando o navio a rotas perigosas, ou até mesmo ao introduzir dados falsos de GPS (*spoofing*), com o intuito de enganar a tripulação sobre a sua real posição.

2.2.3 *Ransomware* e Ataques a Infraestruturas Críticas.

Infraestruturas críticas, como as do setor marítimo, tornaram-se alvos preferenciais para ataques de *ransomware* devido ao alto impacto de uma paralisação. A interrupção das operações portuárias ou de um navio pode gerar prejuízos milionários e cascatear por toda a cadeia de suprimentos global. Ataques a essas infraestruturas não visam apenas o ganho financeiro, mas também podem ter

motivações geopolíticas, buscando desestabilizar economias ou nações. Segundo o Instituto Brasileiro de Logística (IBL, 2025), a crescente digitalização e interconectividade, embora tenha aumentado a eficiência operacional, trouxe um aumento na superfície de ataque no espaço digital. Para entender o risco, é preciso definir o que é uma IC.

Conforme o decreto n° 9.573, promulgado em 22 de novembro de 2018, a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), as define da seguinte forma:

> Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade'; e a segurança de infraestrutura críticas como: 'conjunto de medidas, de caráter preventivo e reativo, destinados a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas

A partir dessa definição, é possível estabelecer que o setor de transporte marítimo se enquadra como um Infraestrutura Crítica. Conforme informações retiradas da Royal United Services Institute (RUSI, 2024), a interrupção pode causar consequências desastrosas, conforme apresentado na tabela a seguir:

Tabela 3: Impacto de interrupções no setor marítimo

Tipo de Impacto	Descrição
Econômicos e Comerciais	Perturbação das cadeias de abastecimento e paralisação do comércio global.
Econômicos e Comerciais	Perda de receita financeira e reputação das organizações.
Operacionais e Logísticos	Danificação ou desativação de dispositivos mecânicos críticos.
Operacionais e Logísticos	Paralisia do navio e roubo ou desvio de carga.
Segurança Humana e Ambiental	Risco de ferimento de trabalhadores.
Segurança Humana e Ambiental	Falha de sistemas inteligentes de detecção e combate de incêndio.
Segurança Humana e Ambiental	Derrame de combustível e outros poluentes em ambiente marítimo.
Segurança Nacional e Soberania	Entrada de armas, drogas, tráfico humano ou atos de terrorismo.
Segurança Nacional e Soberania	Utilização dos sistemas de segurança para espionagem estrangeira.

Fonte: Autoria Própria, baseada em RUSI (2024)

Levando em conta a seriedade dos impactos citados na tabela 3, é imprescindível que o setor marítimo obtenha uma proteção sólida contra ameaças externas. Na atualidade, o ciberataque é um dos métodos mais disruptivos em larga escala. Dentre as diversas categorias de ameaças cibernéticas, o *ransomware* se destaca pelo seu alto poder destrutivo e pela capacidade de paralisar operações na sua totalidade.

3. METODOLOGIA DE PESQUISA

Este capítulo descreve os procedimentos metodológicos adotados para responder à pergunta de pesquisa e atingir os objetivos propostos. A metodologia define a abordagem lógica e sistemática que fundamenta a coleta, a análise e a interpretação dos dados, assegurando o rigor científico e a validade dos resultados apresentados.

Esta pesquisa é de natureza qualitativa, pois o estudo não se concentra em quantificar dados ou em análises estatísticas, mas sim em compreender e interpretar um fenômeno complexo: o impacto de um ataque de *ransomware* em uma infraestrutura crítica marítima. O foco está na análise aprofundada do contexto, das falhas de governança e dos processos técnicos que levaram ao incidente, bem como na extração de lições subjetivas e contextuais.

Já quanto aos objetivos, esta pesquisa classifica-se como exploratória e descritiva. É exploratória por buscar maior familiaridade com o problema, que envolve cibersegurança, tecnologia operacional e o setor marítimo, uma área ainda em desenvolvimento no debate acadêmico nacional. O estudo visa aprofundar o conhecimento sobre as vulnerabilidades específicas deste setor. A pesquisa também é descritiva ao detalhar as características do incidente da Maersk, descrevendo a cronologia dos eventos, os vetores de ataque do *malware* NotPetya, os impactos operacionais e financeiros, e as respostas da empresa. Adicionalmente, descreve o cenário regulatório e tecnológico da frota marítima brasileira para contextualizar a aplicação das lições aprendidas.

Quanto aos procedimentos técnicos, esta pesquisa combina a pesquisa bibliográfica, a pesquisa documental e o estudo de caso como estratégias centrais. Os procedimentos foram divididos em duas frentes principais: a fundamentação teórica e a análise empírica do caso selecionado.

A primeira etapa consistiu em uma ampla revisão de literatura para construir o referencial teórico (Capítulo 2). Conforme Gil (2008), a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, como livros e artigos científicos. Além disso, segundo o mesmo autor (Gil, 2008), a pesquisa documental utiliza fontes que

ainda não foram submetidas a uma análise científica, como relatórios e documentos oficiais.

As fontes utilizadas incluíram fontes bibliográficas, como artigos acadêmicos de bases de dados como Scielo e Google Scholar; livros de referência sobre cibersegurança e gestão de riscos; teses e dissertações sobre o tema. Foram utilizadas também fontes documentais, como relatórios técnicos de empresas de segurança da informação sobre o ataque NotPetya; publicações oficiais da Organização Marítima Internacional (IMO), como a Resolução do Comitê de Segurança Marítima MSC.428(98); documentos do governo brasileiro, como a Estratégia Nacional de Cibersegurança (E-Ciber) e a Política Nacional de Cibersegurança (PNCiber); além de artigos de imprensa especializada que cobriram o incidente da Maersk.

3.1 Estudo de Caso

O ponto central desta pesquisa é o estudo de caso, que, segundo (Yin, 2015), é uma investigação empírica que examina um fenômeno contemporâneo em profundidade e em seu contexto de mundo real. O ataque de *ransomware* à A.P. Moller-Maersk em 2017 foi selecionado como um caso crítico, pois representa um evento que expôs de forma dramática as vulnerabilidades do setor marítimo global à guerra cibernética, servindo como um ponto de inflexão para a indústria. A análise do estudo de caso seguiu as seguintes etapas, baseadas nos princípios de Yin (2015):

- Planejamento: Definição da pergunta de pesquisa e dos objetivos do estudo.
- Coleta de Dados: Levantamento de informações a partir das fontes documentais para reconstruir a cronologia do ataque, identificar as falhas técnicas e de governança, e documentar as consequências.
- Análise dos Dados: Análise qualitativa das informações coletadas para extrair as principais lições técnicas (p. ex., segmentação de rede, planos de *backup*) e de governança (p. ex., gestão de riscos integrada TI/TO, plano de resposta a incidentes).

- Elaboração do Relatório: Apresentação dos resultados da análise nos capítulos subsequentes, conectando os achados do caso com o referencial teórico e as recomendações para o contexto brasileiro.

3.2 Limitações da Pesquisa

É importante reconhecer que este trabalho se limita à análise de fontes secundárias e dados publicamente disponíveis. Devido à natureza sensível das informações sobre segurança cibernética e à impossibilidade de acesso direto aos sistemas e equipes da Maersk ou de empresas da frota brasileira, não foi realizada a coleta de dados primários (como entrevistas ou análises de sistemas *in loco*). Portanto, as conclusões e recomendações baseiam-se na interpretação e síntese das informações documentadas e disponíveis publicamente sobre o evento e o setor.

4. ESTUDO DE CASO: A ESTRATÉGIA DE RECUPERAÇÃO DA MAERSK

Este capítulo se dedica ao estudo de caso da A.P. Moller-Maersk. A análise do caso permite aplicar conceitos teóricos de vulnerabilidade e propagação de ameaças a um cenário real, destacando as falhas de governança e ausência de planos que foram expostos. O capítulo examina a cronologia do ataque, os impactos e o processo de recuperação da empresa, a fim de extrair lições para a mitigação de riscos no contexto brasileiro.

4.1 O contexto geopolítico do ataque NotPetya.

O NotPetya surgiu em 27 de junho de 2017 na Ucrânia. De acordo com Grasso (2024), essa data foi escolhida de forma estratégica, pois coincidia com o Dia da Constituição, um feriado nacional no país. Isso permitiu que o ataque fosse mais ostensivo, tendo em vista que a maioria dos funcionários, inclusive os da área segurança cibernética, estavam de folga no dia.

Outro motivo apontado para a escolha da data, está intrinsecamente ligado a gerar maior instabilidade política, ou seja, um ataque simbólico à soberania ucraniana.

No dia 02 de julho de 2017, a British Broadcasting Corporation (BBC) anunciou uma declaração da inteligência ucraniana, no qual indicou ter encontrado provas de que a Rússia estava por trás do ataque. Moscou negou qualquer envolvimento com o incidente e declarou que essas provas seriam infundadas. Apesar disso, Grasso (2024) aponta que posteriormente nações como Estados Unidos, Reino Unido e Ucrânia atribuíram a responsabilidade do ataque à Rússia e condenaram-na de forma pública.

4.2 Análise Técnica do NotPetya: Vetores de Infecção, Propagação e Carga Útil.

O vetor inicial de infecção do NotPetya foi o *software* de contabilidade ucraniano chamado MeDoc, que era utilizado por aproximadamente um milhão de empresas no país, inclusive por instituições governamentais. De acordo com a empresa de Cibersegurança Talos (Krasznay, 2020), no dia 24 de abril de 2017 foi

liberada uma atualização do aplicativo contendo um *backdoor*, que foi o propulsor do ataque ocorrido em junho do mesmo ano.

Segundo Grasso (2024), o NotPetya infecta o Registro Mestre de Inicialização (*Master Boot Record* - MBR), do computador, responsável por carregar o sistema operacional. Uma vez dentro de uma rede, o NotPetya demonstrou uma capacidade destrutiva de propagação lateral. Para isso, ele utilizou duas ferramentas conhecidas:

- Eternal Blue: aplicação roubada da Agência de Segurança Nacional (NSA) dos Estados Unidos, capaz de encontrar vulnerabilidades no sistema operacional Windows e executar códigos no dispositivo.
- Mimikatz: criada pelo pesquisador francês Benjamin Delpy em 2011, para coleta de credenciais de administrador e foi utilizada para acessar outras máquinas na rede.

Grasso (2024) também aponta que inicialmente, o NotPetya invade a rede através do MeDoc e procura computadores vulneráveis à falha do Windows contra o EternalBlue, ao fazê-lo ele utiliza o Mimikatz para coletar a credencial de administrador e por fim infectar outras máquinas dentro da rede em alta velocidade. Os impactos do NotPetya foram tão significativos que ao atingir à Maersk, levou apenas 7 minutos para se espalhar pela rede global da empresa.

Essa velocidade de propagação foi consequente da falta de segmentação de rede. Sem a divisão da topologia de rede por objetivo e segurança, o *malware* não foi limitado à filial ucraniana de empresas como a Maersk. Um exemplo desse impacto foi a paralisação das atividades no porto de Itajaí, no estado de Santa Catarina, onde os contêineres operados pela APM Terminals, subsidiária do grupo Moller-Maersk, foram afetados pelo NotPetya.

Não apenas o código apresentava semelhanças com o *ransomware* Petya, mas toda a sua *interface* foi feita para confundir os funcionários e atrasar a resposta ao ataque. Como pode ser visto na figura 1, que imita a *interface* do Petya.

Figura 1: Interface de computadores infectados

Fonte: Kaspersky (2017)

4.3 Ransomware ou *wiper*?

Em conformidade com o que foi abordado na seção anterior, a principal motivação de um ataque *ransomware* é o ganho financeiro. Todavia, segundo Krasznay (2020), o principal fator que o diferencia de outros tipos de *malware*, reside no fato de que o *e-mail* fornecido para o pagamento do resgate era falso, logo não havia nenhuma forma de recuperar os dados perdidos. Levando isso em conta, a principal motivação do ataque não visava ganhos financeiros, mas sim a sabotagem em massa, fundada em objetivos geopolíticos.

Especialistas que analisaram o ataque consolidaram essa natureza de caráter destrutivo. De acordo com Oleh Derevianko, diretor da *Information Systems Security Partners* (2017), o que tornou o NotPetya tão distinto e até mesmo assustador, se deve ao fato de tudo o que ocorreu durante o ataque, parecia automatizado, com o intuito de enganar as suas vítimas, e por consequência, enfraquecer a defesa. (Borys, 2017).

4.4 O processo de restauração

A empresa de consultoria Deloitte, sediada em Londres, foi contratada para o gerenciamento da recuperação. Porém havia um problema, os arquivos de *backup* foram programados para que qualquer um deles funcionasse para restaurar os outros. Entretanto, o que não foi considerado nesse caso, foi a possibilidade de todos esses arquivos fossem deletados simultaneamente.

Vale destacar que antes do ataque ocorrer, um dos escritórios da Maersk sediado em Gana tinha sofrido com uma queda de energia, com isso, todas as máquinas se desconectaram da rede. Apesar disso ser algo positivo, a Internet desse escritório remoto era limitada, estima-se que o controlador de domínio tinha centenas de *gigabytes*, e com a conexão local, levaria dias para que fossem transferidos.

Diante desse obstáculo a solução foi levar a mídia física do *backup* a Londres. Um funcionário de Gana viajou para a Nigéria para entregar o disco rígido contendo o controlador de domínio, um servidor que responde a requisições de autenticação, para um outro empregado, que por sua vez, voou para Londres, onde a Deloitte estava gerenciando a recuperação, entregando a peça essencial para a reconstrução da empresa.

Pownall (2019) destaca que, embora tenham conseguido resolver a pausa de dez dias nos serviços da empresa, houve perdas financeiras estimadas entre 200 e 300 milhões de dólares, além da necessidade de reinstalar 4000 servidores e 45000 computadores pessoais. Essa operação de recuperação, que dependeu de um esforço improvisado e manual, expôs o custo da falha de governança e ausência de políticas de *backup* robustas podem causar.

5. ANÁLISE E RECOMENDAÇÕES PARA O CONTEXTO BRASILEIRO.

O presente capítulo será dedicado a abordar as principais lições que foram aprendidas com o incidente da Maersk aplicados ao contexto nacional. Inicialmente será apresentado o cenário regulatório e estratégico, com ênfase na Resolução MSC.428(98) da IMO e na Estratégia Nacional de Cibersegurança (E-Ciber) que fundamentam a base para a gestão de riscos. Posteriormente, serão abordadas as principais recomendações técnicas aprendidas com o incidente da Maersk, relacionados à segmentação de redes, políticas de *backup offline* e outros métodos de proteção, como o uso de *firewall* e Virtual Local Area Networks (VLAN). Por fim, serão abordados aspectos relacionados à Governança de TI, como a Gestão de Riscos Integrada, as políticas de controle de acesso para usuários, funcionários e visitantes, aliados a um plano de resposta a incidentes claro e bem definido, a fim de coordenar ações de recuperação eficazes.

5.1 Cenário regulatório e estratégico

Após a análise da ameaça NotPetya e da superfície de ataque do setor marítimo, este capítulo se dedica a examinar as respostas estratégicas e regulatórias a essas vulnerabilidades. Para isso será abordado em duas frentes: a resposta internacional, com o foco na Resolução MSC.428(98) da IMO, e a perspectiva nacional, que analisa a Estratégia Nacional de Segurança Cibernética (E-Ciber).

5.1.1 A Resposta Internacional: Resolução MSC.428(98) da IMO

Adotada pela IMO em junho de 2017, a resolução MSC.428(98) foi uma resposta direta à crescente ameaça cibernética no setor. Sua adoção foi acelerada pelo ataque NotPetya, ocorrido nesse mesmo período, que expôs as vulnerabilidades operacionais do setor em larga escala. A urgência dessa medida foi confirmada pela tendência de alta nos anos seguintes, que registraram um aumento de 900% em ciberataques entre 2018 e 2021 (Freire, 2024)

Ao adotar a resolução, a IMO reconheceu a urgência de elevar a consciência situacional sobre riscos e vulnerabilidades cibernéticas. De acordo com Castro (2021

apud Coelho Júnior; da Silva 2024), a resolução estabeleceu que a gestão de riscos cibernéticos deve ser integrada aos Sistemas de Gestão de Segurança (SGS) das embarcações, seguindo os requisitos funcionais do Código Internacional de Gestão de Segurança (ISM).

Nesse sentido, Campos (2021) aponta que a segurança cibernética passou a ser coberta pelo Código ISM a partir de 2021, devendo ser parte integrada ao sistema de gestão de segurança das embarcações, inclusive com a adoção de planos de contingência. Para os navios, Oliveira (2022) diz:

> A Diretoria de Portos e Costas (DPC), como representante da Autoridade Marítima Brasileira (AMB), internalizou essa Resolução nas Normas da Autoridade Marítima (NORMAM), especificamente na NORMAM-01/DPC, em que prevê que o Sistema de Gerenciamento de Segurança (SGS) dos navios deverá constar, entre outros itens, de uma abordagem dos riscos cibernéticos, na primeira verificação anual do documento de conformidade da empresa.

Com o Brasil em mente, na próxima seção será abordada a Estratégia Nacional de Segurança Cibernética (E-Ciber) isso porque, como apontado por Oliveira (2022), a Política Marítima Nacional (PMN), publicada em 1994, não institui regras para o ambiente cibernético.

5.1.2 A Perspectiva Nacional: A Estratégia Nacional de Segurança Cibernética (E-Ciber)

A E-Ciber representa o principal documento de orientação do Brasil no campo da cibersegurança. O país avançou muito na política para isso, desde que a defesa cibernética foi considerada um setor estratégico em 2008 (Goldoni, Rodrigues, Medeiros, 2024). Com a priorização do Gabinete de Segurança da Presidência da República (GSI/PR) em 2020, considerando a área mais importante e crítica no momento, como aponta Oliveira (2022), foi criado a E-Ciber.

Nessa primeira publicação foram definidos três objetivos estratégicos que serviram para estabelecer as ações estratégicas visando segurança cibernética:

> 1. Tornar o Brasil mais próspero e confiável no ambiente cibernético;
> 2. Aumentar a resiliência brasileira a ameaças cibernéticas;
> 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional. (Brasil, 2020)

Entre as dez ações estratégicas criadas, foram retirados dois exemplos para trabalhar no parágrafo seguinte:

- Elevar o nível de proteção de Infraestruturas Críticas Nacionais.
- Estabelecer um modelo centralizado de governança no âmbito nacional.

Como aponta Hurel (2021), essas ações carecem de metas claras e de estipular mecanismos de ações estratégicas propostas, além de métricas para avaliação de resultados. Com isso o documento foi duramente criticado e considerado apenas “uma carta de boas intenções do governo brasileiro”.

Em 4 de agosto de 2025, foi instituída pelo decreto 12.573 uma nova versão, proposta pelo Comitê Nacional de Cibersegurança (CNCiber). Entre as principais características e objetivos, destacam-se as novas áreas abordadas como parte da conscientização da população

De acordo com Goldoni, Rodrigues e Medeiros (2024), a E-ciber também se insere dentro do arcabouço normativo, ou seja, um conjunto de normas que se organiza em diferentes divisões, conforme apresentado na tabela 4.

Tabela 4: Divisão da E-Ciber

Nível	Explicação
Político	Coordenado pelo GSI/PR, abrange a Administração Pública Federal (APF) e ICs
Estratégico	Em função do Ministério da Defesa, do Estado-Maior Conjunto das Forças Armadas e dos Comandos das Forças Armadas, com base na Doutrina Militar de Defesa Cibernética
CNCiber	Colegiado liderado por um representante do GSI/PR que orienta a cibersegurança do país e propõe atualizações para políticas e plano nacionais
Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)	Instituída pelo Decreto n° 10.748/2021, busca melhorar a coordenação para prevenção, tratamento e resposta a incidentes na Administração Pública Federal.

Fonte: Autoria Própria, baseado em Brasil (2023).

Apesar do desenvolvimento recente, o Brasil apresenta vários documentos que, por vezes, são desconexos e de maturidade obscura (Goldoni, Rodrigues, Medeiros 2024). Além disso, como aponta Oliveira (2022), embora a questão de IC seja abordada pela E-Ciber, ela carece de estratégias e diretrizes cibernéticas para o setor marítimo.

No dia 26 de dezembro de 2023 foi promulgado o decreto nº 11.856, que instituía a Política Nacional de Cibersegurança (PNCiber), ela tinha como objetivo orientar a atividade de segurança cibernética no país, além de unificar a “colcha de retalhos” regulatória existente, ou seja, integrando ações anteriores como a PNSIC ou a Política Nacional de Segurança da Informação (PNSI).

Apesar da ideia inicial, isso não se concretizou de fato na política que foi promulgada, já que ela sequer menciona órgãos reguladores já existentes, como a E-ciber e a ReGIC, por exemplo, levando a conclusão de que essas ações não seriam integradas de forma eficaz na presente política.

Além disso, Goldoni, Rodrigues e Medeiros (2024) apontam que a PNciber não possui verba e nem mão de obra para sair do papel, e essa ideia é reforçada quando se considera a minuta da política, que previa a criação de uma Agência Nacional de Cibersegurança (ANCiber), que contaria com 800 servidores e 300 cargos comissionados, responsáveis pela execução da PNCiber, entretanto, esse órgão sequer é mencionado na versão que foi promulgada, evidenciando a dificuldade de financiamento.

Diante do cenário regulatório exposto, que demanda uma gestão de riscos mais sólida, as seguintes lições técnicas extraídas do caso da Maersk tornam-se imprescindíveis à frota marítima brasileira.

5.2 Lições técnicas aprendidas com à Maersk

Em conformidade com o que foi apresentado no subcapítulo 4.2, o principal vetor que permitiu a propagação do NotPetya em escala global foi a ausência de segmentação de redes. Essa ideia é reforçada por Steinberg, Stepan e Neary (2021), no qual se ressalta que os impactos poderiam ser reduzidos drasticamente, caso as máquinas da Maersk não estivessem conectadas à mesma rede. No que diz respeito à frota marítima brasileira, essa lição se traduz diretamente na necessidade de revisão das arquiteturas de rede a bordo, com o intuito de garantir que os sistemas de TO estejam separados das redes administrativas de TI.

Levando isso em conta, essa vulnerabilidade viola diretamente a função ‘Proteger’ (PR) do *framework* NIST, de forma específica a subcategoria PR.IR-01, no qual se determina que as redes e ambientes devem ser protegidos contra uso e

acesso não autorizado no âmbito lógico. Em adição a isso, a *Baltic and International Maritime Council* (BIMCO *et al*., 2024) apresenta uma série de recomendações básicas e práticas referentes a segmentação de redes, dentre elas destacam-se

1. Comunicação necessária entre os equipamentos de TO, além da sua configuração e monitoramento.
2. Tarefas administrativas a bordo, incluindo *e-mail*, arquivos compartilhados ou pastas relacionadas, por exemplo: administração do navio, operações de carga, gerenciamento técnico (redes de TI), etc.
3. Acesso recreativo para tripulação e passageiros ou visitantes.
4. Redes para navegação e redes para maquinário de carga.
5. Segmento de conexão sem fio (*wireless*) na rede TO.
6. Equipamentos de segurança na rede TO e nos seus demais segmentos

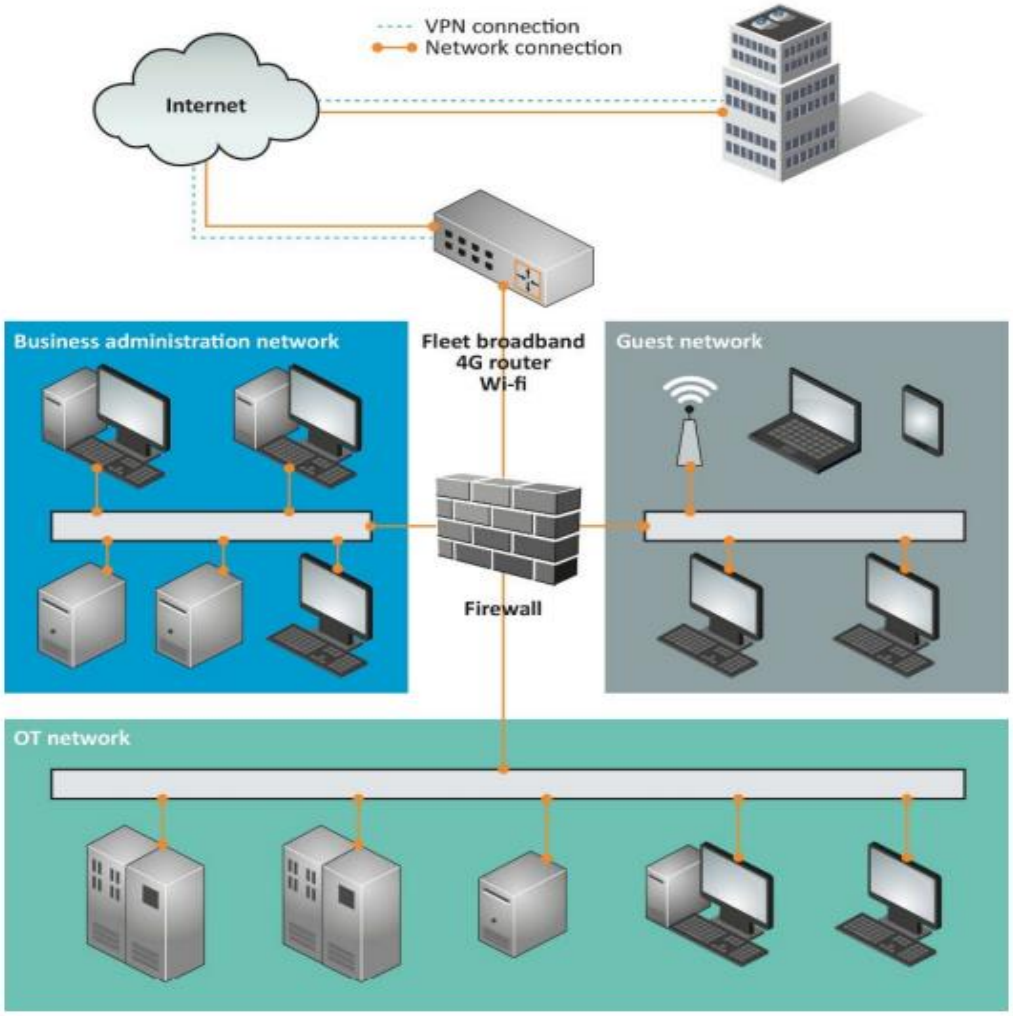
5.2.1 Implementação lógica com VLANs.

Perante o que foi abordado acima, em relação aos procedimentos básicos de segmentação de redes, a fim de implementá-la de forma prática, destaca-se o uso de VLANs, que pode ser definida da seguinte forma:

> Como o nome já sugere, um comutador que suporta VLANs permite que diversas redes locais virtuais sejam implementadas através de uma única infraestrutura física de uma rede local virtual. Hospedeiros dentro de uma VLAN se comunicam como se eles (e não outros hospedeiros) estivessem conectados ao comutador. Em uma VLAN baseada em pontos, as interfaces do comutador são divididas em grupos pelo gerente da rede. Cada grupo constitui uma VLAN, com as interfaces em cada VLAN formando um domínio de broadcast (por exemplo, o tráfego de broadcast de uma interface só pode alcançar outras interfaces no grupo). (Kurose; Ross. 2010, p. 355-356)

Conforme detalhado pelo guia da BIMCO *et al*. (2024) o uso de VLANs pode ser aplicado para hospedar os segmentos da rede de forma isolada, sendo que cada um desses segmentos deve conter a sua própria faixa de endereços *Internet Protocol* (IP), afinal a segmentação de rede não anula a necessidade de configurações adequadas em cada segmento, especialmente em relação a controles de acesso bem definidos, *softwares* de *firewall* e detecção de *malware*. A figura 2 ilustra de forma prática as medidas apresentadas acima:

Figura 2: O Uso de VLANs para segmentação de rede



Fonte: BIMCO *et al,* 2024

Conforme apresentado na figura 2, o documento técnico da BIMCO *et al*. (2024) recomenda que sejam criados segmentos de redes distintas, a fim de isolar os sistemas críticos do navio, como maquinários e sistemas de operação, presentes na rede de TO, das tarefas administrativas (TI). Ademais, visando uma proteção mais restrita, destaca-se a necessidade de separação da rede da tripulação e da rede dos visitantes, tendo em vista que essas redes não são gerenciadas e que as informações referentes a segurança, como antivírus e atualizações são desconhecidas. Essa medida é crucial para a proteção das infraestruturas críticas do navio, principalmente ao considerar que os usuários destas redes podem estar agindo de maneira maliciosa, seja de forma intencional ou não. Cabe mencionar que essa divisão deve abranger os equipamentos de segurança e conexões sem fio dentro da própria rede operacional.

5.2.2 Controle e Monitoramento com *Firewalls*.

Em complemento às práticas de segmentação apresentadas, vale destacar que para que a segurança cibernética seja efetiva, é imprescindível que outras medidas complementares sejam adotadas. Conforme exposto por Freire (2024), entre as melhores práticas mais difundidas, destacam-se o uso de *firewall* e sistemas de detecção de intrusão, em acréscimo a realização de auditorias frequentes, a fim de expor novas fragilidades existentes ou brechas de segurança que não foram identificadas previamente. Loureiro (2016) acrescenta que para além do uso de *firewalls*, é fundamental reforçar as capacidades de segurança cibernética, com ênfase na gestão de riscos aliada à análise de vulnerabilidades presentes em todos os sistemas geridos por *software*.

Com o intuito de implementar esses métodos de forma prática e alinhados às melhores práticas globais, organizações como a BIMCO e o NIST estabelecem diretrizes, que oferecem um roteiro detalhado dessa implementação.

Conforme detalhado pelo guia da BIMCO *et al.* (2024), em alinhamento à subcategoria PR.IR-01 do *framework* NIST, se estabelece que para assegurar a segurança, redes de TO em específico devem ser fisicamente segmentadas das redes de TI e das redes públicas. Dentre algumas das medidas de proteção que podem ser utilizadas, destacam-se o uso de um *firewall* por perímetro entre as redes de bordo e a Internet, para o controle de tráfego entre esses dois segmentos, o uso de *switches* para cada segmento da rede, além de *firewalls* internos entre cada segmento da rede.

Por fim, para garantir a efetividade das configurações de VLANs, é imprescindível o uso de *firewalls* de perímetro, que são utilizados para proteger os limites de uma rede ou sistema, garantindo que caso haja atividade maliciosa em um dos segmentos, o atacante não consiga transpor os limites definidos e acessar os demais segmentos. Esse procedimento é fundamental para garantir a segurança de segmentos críticos de uma organização.

5.2.3 *Backup offline*

Conforme o que foi apresentado no subcapítulo 4.4, o principal fator que influenciou no processo de recuperação da Maersk, está diretamente ligado a uma queda de energia de um escritório da empresa em Gana, que devido a ter sido desconectado da rede anteriormente a propagação do NotPetya, conseguiu manter de forma íntegra um disco rígido com o *backup* da organização. Porém, vale salientar que esse evento foi um acontecimento isolado e uma coincidência favorável, portanto, embora isso tenha favorecido o processo de recuperação, não pode ser utilizado como métrica de boas práticas de *backup*.

Em adição ao exposto, referente ao contexto brasileiro, conforme apresentado no relatório do Tribunal de Contas da União (TCU), realizado no ano de 2022, aproximadamente 73,1% dos serviços do Governo federal dependem de forma exclusiva de plataformas digitais, já em relação aos que dependem dessa instância de forma parcial, o número aumenta para 83,7%. Além disso, estima-se que 74,6% dos órgãos públicos não possuem uma política de *backup* estabelecida, e entre os que possuem, aproximadamente 66% não empregam a criptografia para proteção dos seus dados (TCU, 2022).

Diante do exposto, a BIMCO *et al*. (2024) recomenda o uso de *backup offline*, que consiste no armazenamento dos principais *backups* em um disco rígido, que esteja desconectado da rede, já que historicamente ataques de *ransomware* e *worms* se espalharam em dispositivos de *backup*.

Essa sugestão está intrinsecamente alinhada com a subcategoria PR.DS-11 do *framework* NIST, que estabelece que os *backups* de dados são criados, protegidos, mantidos e testados.

5.3 Governança de TI: Gestão de Riscos Integrada (GRI) e Plano de Resposta a Incidentes (PRI)

O ataque à Maersk demonstrou que as vulnerabilidades mais catastróficas não são apenas de *software*, mas também de governança. A falta de estrutura de gestão de riscos unificada e a ausência de um plano de resposta transformaram uma infecção localizada em um colapso global. As recomendações de governança para o setor

marítimo brasileiro devem se concentrar em institucionalizar a segurança cibernética no nível executivo e planejar a continuidade de negócio diante de uma perda total de sistemas.

Conforme mencionado anteriormente no capítulo 4.4, o fato da AP Moller-Maersk depender de forma exclusiva de um único *backup* em Gana evidencia uma falha crítica de governança e planejamento. Essa negligência em relação a gestão de riscos e um plano de resposta a incidentes é ilustrada de forma tangível nos custos referentes aos prejuízos causados por essa falha, estimado entre 200 e 300 milhões de dólares.

A principal alternativa em relação à essa lacuna, segundo Polemi e Maele (2024) está presente na Gestão de Riscos Integrada (GRI), que trata a Segurança Cibernética de uma forma holística e não fragmentada, ou seja, essa abordagem deve levar em conta tanto os aspectos físicos de um navio, como os cibernéticos.

A aplicação dessa GRI se dá na Resolução MSC.428(98) da IMO, que segundo Oliveira (2022) foi internalizada nas Normas da Autoridade Marítima (NORMAM), em específico na NORMAM-01/DPC, no qual se estabelece que a partir de 1º de janeiro de 2021, O SGS, isto é, o *framework* responsável pelo gerenciamento das operações de segurança a bordo, deve abordar os riscos cibernéticos no setor. Em complemento à essa norma, no dia 22 de novembro de 2018, através do Decreto nº 9.573 foi aprovada a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), ou seja, uma estratégia do Estado brasileiro para garantir a proteção de serviços essenciais, como energia, transporte e finanças, que está diretamente relacionada a segurança e a resiliência das infraestruturas críticas, além da sua continuidade na prestação de serviços.

Dentre os principais fundamentos dessa política, destacam-se o uso da análise de riscos como base para a prevenção e resiliência, aliada a integração entre diferentes setores do Poder Público, ou seja, desde o setor empresarial até os demais segmentos da sociedade.

Vale destacar que apesar da existência dessa política, Oliveira (2022) aponta que não existe nenhum guia prático, com orientações de segurança cibernética destinados a Navios, Portos e Instalações Portuárias, algo já existente no Reino Unido, conforme exposto pelo autor.

A fim de aplicar essa abordagem de forma prática, destacam-se algumas práticas e procedimentos, dentre as ações mais básicas, como tornar a segurança cibernética parte da cultura da organização, através de treinamentos e seminários, com exercícios referentes a todos os níveis de segurança, além de incentivar o compartilhamento de informações e a colaboração, ou seja, a incentivar que os colaboradores informem sobre atividades suspeitas, seja essa ação algo externo, como um incidente ou interno, como uma violação das políticas de segurança por outro colaborador.

Outras práticas desse nível incluem um controle de acesso eficaz, além de políticas de autenticação e de palavra passe, ou seja, estabelecer que as senhas de cada colaborador devem conter um número mínimo de caracteres, combinando diferentes elementos, como letras maiúsculas, minúsculas, números e símbolos.

Já no nível mais estratégico, destacam-se as seguintes medidas: o passo inicial é a classificação de ativos, afinal uma organização não pode proteger o que desconhece. Para a frota marítima isso se traduz no mapeamento e hierarquização dos sistemas de TI e TO, abordando desde as redes administrativas aos sistemas críticos de navegação e maquinário, definindo desta forma o impacto no negócio caso haja uma falha em cada um deles.

Essa etapa é fundamental na criação de um Plano de Resposta a Incidentes (PRI) eficaz, pois ao conhecer quais ativos são os mais críticos a bordo, a organização pode definir prioridades claras e objetivas para contenção e recuperação, garantindo que no caso de um cenário de crise como o que afligiu a Maersk, os esforços sejam aplicados a recuperar as funções vitais da embarcação. A criação de planos desse tipo no Brasil é estimulada pela Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), que busca melhorar a coordenação para prevenção, tratamento e resposta a incidentes cibernéticos na Administração Pública Federal e serve de modelo de gestão para IC.

No nível operacional, a eficácia do PRI exige a classificação de ativos críticos, conforme o relatório da RUSI (2024), essa etapa é essencial, pois permite o mapeamento e hierarquização dos sistemas de TI e TO. Ao conhecer quais ativos são mais críticos, a organização pode definir prioridades claras para contenção e recuperação, garantindo que em um cenário de crise, os esforços sejam aplicados

primeiramente para restaurar as funções vitais, seja de uma organização, porto ou embarcação.

Em resumo, a lição com a Maersk, agora comprovada pela análise das diretrizes nacionais e internacionais, é que a resistência cibernética no setor marítimo não é um problema de tecnologia, mas de governança e arquitetura. A proteção da frota brasileira requer a aplicação integrada das recomendações aqui analisadas: a segmentação física de rede deve ser sustentada por uma GRI, garantindo a supervisão executiva, e por um PRI que contemple cenários de perda total.

6. CONSIDERAÇÕES FINAIS

O presente trabalho teve como objetivo analisar os impactos do ataque de *ransomware* NotPetya à A.P. Moller-Maersk, ocorrido em 2017, e extrair lições aplicáveis à proteção da frota marítima brasileira. A partir da revisão bibliográfica, da pesquisa documental e do estudo de caso, foi possível compreender que a crescente digitalização do setor marítimo, embora proporcione eficiência e inovação, também amplia significativamente a superfície de ataque cibernético, expondo embarcações e portos a riscos críticos.

Vale destacar que o terceiro objetivo específico do trabalho, ‘Identificar vulnerabilidades da frota marítima brasileira’ foi parcialmente cumprido, devido à insuficiência de dados públicos sobre esse tópico, algo que está diretamente ligado a questões de segurança. Conforme apontado por Oliveira (2022), a própria lista de Infraestruturas Críticas Marítimas (ICM) é classificada como de caráter sigiloso pelo GSI, e consequentemente não pode ser divulgada. Diante dessa limitação, a análise se limitou a vulnerabilidade mais evidente e documentada: a lacuna na governança.

De forma paralela, através da análise do cenário regulatório brasileiro, foi identificado um esforço contínuo para a criação de um arcabouço normativo, que culminou na recente Política Nacional de Cibersegurança (PNCiber) de 2023. Entretanto, Goldoni, Rodrigues e Medeiros (2024) apontam que essa política possui uma estrutura desconexa e uma carência de ferramentas de políticas públicas eficazes, para que seja implementada de forma efetiva. Essa ideia reforça a crítica de Oliveira (2022) no qual é mencionada a ausência de guias e diretrizes específicos para infraestruturas marítimas no Brasil.

Diante disso e levando em conta o estudo de caso da Maersk, foi demonstrado que a principal vulnerabilidade não se limita ao *software* utilizado, mas está diretamente ligada à ausência de segmentação de redes, à inexistência de uma governança integrada de riscos e à falta de políticas eficazes de *backup*. Esses fatores transformaram um incidente localizado em um colapso global, que paralisou operações e gerou prejuízos estimados entre 200 e 300 milhões de dólares.

Tendo isso em vista, o trabalho apresentou recomendações voltadas ao contexto brasileiro, enfatizando a necessidade de segmentação lógica de redes por

meio de VLANs, implementação de firewalls e sistemas de monitoramento, utilização de políticas de backup offline, além da inserção da gestão de riscos cibernéticos no nível estratégico das organizações marítimas. Também foi destacada a importância da integração das normas internacionais, como a Resolução MSC.428(98) da IMO, com os instrumentos nacionais, como a Estratégia Nacional de Segurança Cibernética (E-Ciber).

Dessa forma, conclui-se que a mitigação de riscos cibernéticos no setor marítimo brasileiro depende menos da aquisição de novas tecnologias e mais da adoção consistente de boas práticas de arquitetura de rede, aliadas a políticas de governança robustas e a planos de resposta a incidentes. A aplicação dessas medidas pode aumentar a resiliência da frota nacional frente a ataques cibernéticos, reduzindo a dependência de fatores externos e fortalecendo a soberania digital do Brasil.

Como sugestão para pesquisas futuras, recomenda-se a realização de estudos empíricos junto a operadores portuários e empresas de navegação no Brasil, a fim de identificar de forma prática as lacunas existentes na gestão de riscos cibernéticos. Em adição a isso, é sugerido o acompanhamento da implementação da nova Estratégia Nacional de Cibersegurança, derivada da PNCiber, com o objetivo de validar se as lacunas de diretrizes específicas para o setor marítimo serão finalmente supridas.

REFERÊNCIAS

ABNT. Projeto de Revisão **NBR ISO/IEC 27002**: Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro, RJ: ABNT, jul. 2022.

BIMCO *et al*. **The guidelines on cyber security onboard ships**. 5. ed. *[S.l.*]: BIMCO, 2024. Disponível em: https://www.maritimeglobalsecurity.org/media/g3qlxdaw/2024-11-14-guidelines_on_cyber_security-v5-final.pdf. Acesso em: 24 ago. 2025.

BRASIL. Decreto nº 9.573 de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas Estratégia Nacional de Defesa, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 22 nov. 2018. Seção 1, p. 40. Disponível em: http://www.planalto.gov.br/ ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 23 ago. 2025.

BRASIL. Decreto n. 10.222 de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 05 fev. 2020. Seção 1, p. 6. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419>. Acesso em: 04 out. 2025.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 dez. 2023. Seção 1, p. 2. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 03 out. 2025.

BRASIL. Presidência da República. Decreto nº 12.573, de 4 de agosto de 2025: institui a estratégia nacional de cibersegurança – E-Ciber. Brasília, DF: **Diário Oficial da União**, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 03 out. 2025.

CAMPOS, I. Z. A. A segurança cibernética no direito marítimo: uma análise do dever de proteção de dados. **Cadernos do Programa de Pós-Graduação em Direito – PPGDIR. UFRGS,** v.16, n. 2, 2021. Disponível em: https://seer.ufrgs.br/index.php/ppgdir/article/view/118342. Acesso em: 21 ago. 2025.

CASSELL, A. *The modernization double-edged sword: a look at OT cybersecurity in the maritime industry.* **Signal Magazine**, 2024. Disponível em: https://www.afcea.org/signal-media/disruptive-design-modernization-double-edged-sword-look-ot-cybersecurity-maritime. Acesso em: 03 out. 2025.

COELHO JÚNIOR, A; SILVA, L. A cibersegurança na perspectiva do direito marítimo e portuário considerando a evolução tecnológica. **Revista de Direito e Negócios Internacionais da Maritime Law Academy – International Law and Business Review**, 2024. Disponível em: https://mlawreview.emnuvens.com.br/mlaw/article/view/122/205. Acesso em: 23 ago. 2025.

FORTINET. **O que é ransomware?** Como evitar ataques de ransomware?. Fortinet, 2024. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/ransomware. Acesso em: 03 out. 2025.

FREIRE, W. Vista do Cibersegurança Naval: navegando em águas turbulentas na era da Guerra Cibernética. **Revista da Marinha do Brasil**, 2024. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/vitorianassombras/article/view/5950/5678. Acesso em: 03 maio 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

GOLDONI, L.; RODRIGUES, K.; MEDEIROS, B. Qual é o futuro da governança de cibersegurança no Brasil? **Cadernos Gestão Pública e Cidadania**, 2024. Disponível em: https://www.scielo.br/j/cgpc/a/c4LDbpvrpfPhzhQyJRX67NN/?format=pdf&lang=pt. Acesso em: 24 ago. 2025.

GRASSO, G. ***Cybersecurity and the protection of maritime critical Infrastructures.*** 2024. Dissertação (Mestrado em Segurança e Relações Internacionais) – Università di Genova, Gênova, 2024. Disponível em: https://unire.unige.it/bitstream/handle/123456789/9534/tesi30286625.pdf. Acesso em: 21 ago. 2025.

GSI. **Estratégia nacional de Cibersegurança.** Brasília, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber. Acesso em: 24 ago. 2025.

HORDUNA, M.; LĂZĂRESCU, S.-M.; SIMION, E. *A note on machine learning applied in ransomware detection.* **IACR ePrint Archive**, 2023. Disponível em: https://eprint.iacr.org/2023/045.pdf. Acesso em: 02 abr. 2025.

HUREL, L. M. **Cibersegurança no Brasil**: uma análise da estratégia nacional, 2021. Disponível em: https://igarape.org.br/wp-content/uploads/ 2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 4 out. 2025.

IMO**. Resolution MSC.428(98)**: *maritime cyber risk management in safety management systems.* Londres: IMO, 2017. Disponível em: https://wwwcdn.imo.org/localresources/en/OurWork/ Security/Documents/Resolution%20MSC.428(98).pdf. Acesso em: 03 out. 2025.

KASPERSKY. **Como se proteger da nova onda global de ransomware**. Kaspersky 2017. Disponível em: https://www.kaspersky.com.br/blog/new-ransomware-epidemics /9204/. Acesso em: 10 set. 2025.

KASPERSKY. **Tipos de malware e exemplos.** Kaspersky, 2024. Disponível em: https://www.kaspersky.com.br/resource-center/threats/types-of-malware. Acesso em: 03 out. 2025.

KRASZAY, C. Case study: the NotPetya campaign. **Információ- és kiberbiztonság**, 2020. Disponível em: https://www.researchgate.net/profile/Csaba-Krasznay/publication/353072644_Case_Study_The_NotPetya_Campaign/links/60e6

bbe00fbf460db8ee783d/Case-Study-The-NotPetya-Campaign.pdf. Acesso em: 21 ago. 2025.

KUROSE, J.; ROSS, K. **Redes de computadores:** uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010. Disponível em: https://www.facom.ufu.br/~sequincozes/referencias/kurose2010.pdf. Acesso em: 29 set. 2025.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação gerenciais.** 9.ed. São Paulo: Pearson Prentice Hall, 2010.

LOUREIRO, M. V. C. Ataques cibernéticos: ameaças reais ao poder naval. **Revista Marítima Brasileira**, 2016. Disponível em: https://www.portaldeperiodicos.marinha.mil.br/index.php/revistamaritima/article/download/5930/5662. Acesso em: 23 ago. 2025.

MATHEWS, L. *NotPetya ransomware attack cost shipping giant Maersk over $200 million.* **Forbes**, 16 ago. 2017. Disponível em: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/. Acesso em: 21 ago. 2025.

NIST. The NIST cybersecurity framework (CSF) 2.0. Washington, 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 24 ago. 2025.

Organização para Cooperação e Desenvolvimento Econômico (OCDE). **Relatórios de avaliação concorrencial da OCDE: Brasil.** Brasil: OCDE, 2022. Disponível em: https://www.oecd.org/pt/publications/relatorios-de-avaliacao-concorrencial-da-ocde-brasil_283dc7c1-pt.html. Acesso em: 20 fev. 2025.

OLIVEIRA, M. R. **As infraestruturas críticas nacionais ante às ameaças cibernéticas:** análise comparativa das governanças cibernéticas do Brasil e do Reino Unido, com foco nas infraestruturas críticas marítimas. 2022. Tese (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2022.

Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil
.br.egn/files/CPEM%20028.pdf. Acesso em: 23 ago. 2025.

POWNALL, C. **The context and impact of Maerk's NotPetya cyber attack**. 2019. Disponível em: https://www.researchgate.net/publication/346080185_The_
Context_and_Impact_of_Maerk's_NotPetya_cyber_attack. Acesso em: 12 ago. 2025.

RUSI. **Cibersegurança na infraestrutura marítima crítica:** reflexão dos portos africanos. Londres: RUSI, 2024. Disponível em: https://rusieurope.eu/wp-content/uploads/2024/02/cybersecurity-in-maritime-critical-infrastructure-crimson-report-portuguese.pdf. Acesso em: 20 fev. 2025.

STEINBERG, S.; STEPAN, A.; NEARY, K. **NotPetya**: A Columbia University case study. Columbia University, 2022. Disponível em:
https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf. Acesso em: 21 ago. 2025.

TCU. 2022. **Lista de alto risco da administração pública federal:** Segurança da informação e segurança cibernética. Brasília, DF. Disponível em:
https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_
cibernetica.html. Acesso em: 24 ago. 2025.

YIN, R. K. **Estudo de caso:** planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.