UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM ARQUITETURA E GESTÃO DE INFRAESTRUTURA DE TI

EDUARDO DOMANSKI DOS SANTOS

# SEGURANÇA DA INFORMAÇÃO NO AMBIENTE PORTUÁRIO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2021

EDUARDO DOMANSKI DOS SANTOS

# SEGURANÇA DA INFORMAÇÃO NO AMBIENTE PORTUÁRIO

Monografia de Especialização, apresentada ao Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Joilson Alves Júnior

CURITIBA
2021

# TERMO DE APROVAÇÃO

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE PORTUÁRIO

por

EDUARDO DOMANSKI DOS SANTOS

Esta monografia foi apresentada em 20 de Dezembro de 2021 como requisito parcial para a obtenção do título de Especialista em Arquitetura e Gestão de Infraestrutura de TI. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Joilson Alves Júnior
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

# RESUMO

SANTOS, Eduardo Domanski dos. **Segurança da informação no ambiente portuário**. 2021. 21 p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

O presente estudo visa analisar o ambiente portuário sob o aspecto da segurança da informação. A pandemia de COVID-19 trouxe como consequência uma acelerada digitalização dos portos e suas instalações. O desenvolvimento introduzido também veio acompanhado de novas oportunidades aos criminosos: os crimes cibernéticos. Diversas são as vulnerabilidades e as técnicas de exploração, bem como as motivações para os ataques. Espera-se contextualizar a importância da segurança da informação frente ao grande peso econômico que os portos representam para toda a cadeia produtiva internacional. Realiza-se ainda a retomada de conceitos chaves sobre o assunto da segurança da informação, considerados essenciais para o bom entendimento das ameaças eventualmente apresentadas contra as instalações portuárias. Também serão apresentadas algumas ações adotadas no sentido de proteger aquelas infraestruturas e garantir a segurança marítima conforme preconizam as regulamentações internacionais vigentes.

**Palavras-chave:** Cibersegurança. Segurança da Informação. Segurança Portuária. Código ISPS.

## ABSTRACT

SANTOS, Eduardo Domanski dos. **Information security in the port enviroment**. 2021. 21 p. Monografia de Especialização em Arquitetura e Gestão de Infraestrutura de TI, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2021.

The present study aims to analyze the port environment from the point of view of information security. The COVID-19 pandemic has resulted in na accelerated digitalization of ports and port facilities. The development introduced was also accompanied by new opportunities for criminals: cyber crimes. There are several vulnerabilities and exploitation techniques, as well as the motivations for attacks. It is expected to contextualize the importance of information security in view of the great economic weight that ports represent for the entire international production chain. It is also carried out the resumption of key concepts on the subject of information security, considered essential for a good understanding of the threats eventually presented against port facilities. Some actions taken to protect those infrastructures and ensure maritime safety as recommended by current international regulations will also be presented.



**Keywords:** Cybersecurity. Information Security. Port Security. ISPS Code.

## LISTA DE SIGLAS

| | |
|---|---|
| Cesportos | Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis |
| Conportos | Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis |
| CRC | Centro de Resiliência Cibernética |
| IMO | *International Maritime Organization* |
| ISPS Code | *International Ship and Port Facility Security Code* |
| ONU | Organização das Nações Unidas |
| PNSPP | Plano Nacional de Segurança Pública Portuária |

**SUMÁRIO**

# 1 INTRODUÇÃO

As evidências dos primeiros navios construídos na história dão conta que os egípcios foram os precursores da utilização dos mares com a finalidade de comércio. Dedicavam-se à troca de papiros e trigo pelas preciosas madeiras do Líbano, ainda cerca de 3.000 anos antes de Cristo.

A história do comércio marítimo segue ainda com a presença e domínio dos fenícios sobre o Mediterrâneo, posteriormente superados pela hegemonia marítima da Grécia. Por sua vez, os gregos perderam espaço para os romanos, de cujo povo destaca-se o General Pompeu que, sob o lema *navigare necesse est* - navegar é preciso, combateu a pirataria no mar Mediterrâneo.

O monopólio do tráfego marítimo europeu pelas Cidades-Estado bálticas e italianas, o estabelecimento de novas rotas para o oriente em busca das especiarias, a expansão territorial através da colonização de “novos” continentes, entre outros fatos históricos, marcam parte da evolução das relações marítimas internacionais.

Atualmente, a Conferência das Nações Unidas sobre Comércio e Desenvolvimento aponta que pouco mais de 150 países somam 99.800 navios mercantes existentes, os quais são responsáveis pelo transporte de mais de 90% do comércio internacional entre os portos do mundo.

Com tamanha importância, o transporte marítimo requer eficiência, cuja característica depende de ações que facilitem a negociação e o transporte das mercadorias, reduzindo o tempo e custo de procedimentos aduaneiros e comerciais. Nos últimos anos, a introdução de novas tecnologias na administração portuária, como a introdução de serviços de janela única e a digitalização e automação de processos alfandegários, impulsionou o desempenho de toda cadeia logística com efeitos positivos no transporte marítimo. Assim, os atores envolvidos no setor foram encorajados à adoção de soluções propostas pela Tecnologia da Informação.

Desta forma, observa-se que a evolução do comércio marítimo trouxe consigo a evolução dos desafios inerentes à segurança. As ações de pirataria, intensamente combatidas ainda no início da história naval, hoje compartilham espaço com os ciberataques.

## 1.1 TEMA

Este trabalho analisa a segurança da informação, em especial a cibersegurança, no ambiente do comércio marítimo nacional. Ademais, apresenta algumas ações adotadas pelas nações como forma de estabelecer medidas preventivas acerca dos ciberataques.

## 1.2 OBJETIVO

Nesta seção serão apresentados os objetivos geral e específicos do presente trabalho de conclusão de curso.

### 1.2.1 Objetivo Geral

Analisar o cenário da cibersegurança no ambiente portuário nacional e internacional.

### 1.2.2 Objetivos Específicos

Para atender ao objetivo geral deste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

1. Contextualizar a importância da segurança da informação para a segurança portuária.
2. Levantar um breve histórico de ataques ocorridos aos terminais portuários ao redor do mundo.
3. Apresentar as conjunto de medidas produzidos e adotados como referência para garantia da segurança da informação no ambiente portuário.

## 1.3 JUSTIFICATIVA

As tentativas de invasão contra os portos e instalações portuárias tem se tornado uma crescente tendência no cenário internacional. Por esse motivo convém uma análise da importância sobre medidas de se mitigar os riscos de ataques dessa natureza, sejam eles realizados contra terminais públicos ou privados.

## 1.4 METODOLOGIA

A metodologia utilizada é a de pesquisa bibliográfica, a qual foi realizada por meio de pesquisas em livros, manuais e sítios eletrônicos de órgãos oficiais e técnicos especializados, para coleta de uma base para realizar uma explicação do atual cenário.

## 1.5 ESTRUTURA DO TRABALHO

Esta monografia de especialização está dividida em cinco capítulos. No primeiro capítulo foi introduzido o assunto tema do trabalho e também foram abordados a motivação e os objetivos geral e específicos da pesquisa, assim como a justificativa e a estrutura geral do trabalho.

No segundo capítulo, alguns conceitos ligados à segurança da informação são abordados de forma direta, apresentando-se definições encontradas ao longo da literatura sobre o assunto.

A seguir, no terceiro capítulo, o tema da segurança portuária é abordado fazendo-se conexão com o cenário da segurança da informação, em especial a importância da cibersegurança.

No quarto capítulo apresenta-se ciberataques contra terminais portuários nacionais e internacionais que foram registrados nos últimos anos, apontando-se de forma geral as técnicas utilizadas pelos atacantes.

Por fim, no capítulo das conclusões, são apresentadas as considerações finais sobre o assunto.

# 2 SEGURANÇA DA INFORMAÇÃO E OUTROS CONCEITOS

Para Vecchia (2019), a definição de segurança da informação resume-se ao conjunto de medidas que visam tornar as informações mais seguras.

Segurança da Informação (SI) pode ser definida simplesmente como um conjunto de medidas que possuem o objetivo de tornar as informações mais seguras, tendo como alicerce basicamente os seguintes elementos: mecanismos, políticas e cultura. Os mecanismos são implementados via hardware e software, as políticas são baseadas em regras e normas, enquanto a cultura está relacionada ao conhecimento que as pessoas envolvidas possuem (VECCHIA, 2019).

Hintzbergen *et al.* (2018) definem a segurança da informação como a preservação de suas propriedades básicas e destaca a proteção sobre ampla gama de ameaças visando benefícios aos negócios.

Preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem ser incluídas (HINTZBERGEN *et. al*., 2018).

Traduzindo essa definição formal, Hintzbergen *et. al*. (2018) dizem que a segurança da informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

## 2.1 CIBERSEGURANÇA

Dentro do escopo da Segurança da Informação, que visa proteger os ativos de informação, encontra-se a Segurança Cibernética, ou Cibersegurança, que tem seu foco na proteção da informação digital. Para Miller (2016), a cibersegurança consiste na proteção e defesa de sistemas, redes e programas no ciberespaço contra possíveis ataques maliciosos, de forma a se conseguir evitar possíveis danos, sejam estes a nível de *hardware* ou de *software*.

Velho (2016) explica a segurança cibernética vista como estratégia de defesa de âmbito nacional, e sustenta que ela objetiva a proteção dos ativos de informação e suas infraestruturas críticas.

Segundo Velho (2016) o conceito de segurança cibernética pode ser explicado de diversas formas, dependendo de quem o aplica. Porém, é visto por uma nação como a arte de defender a existência e continuidade da informação, de maneira original ou processada, presente no espaço virtual.

A aplicação da segurança cibernética tem o objetivo de proteger os ativos de informação e suas infraestruturas críticas, resguardando os pilares consagrados da segurança da informação, que segundo Velho (2016) são:

a. **Confidencialidade**: garantia que a informação seja acessada ou manipulada apenas por entidades autorizadas;
b. **Integridade**: garantia de que a informação seja mantida com todas as suas características originais, ou modificadas somente pelas partes autorizadas;
c. **Disponibilidade**: garantia que a informação esteja sempre acessível a quem de direito, sempre que preciso;
d. **Autenticidade**: garantia que a informação seja proveniente da fonte indicada.

## 2.2 CIBERAMEAÇAS

Os softwares maliciosos ou *malwares*, combinação das palavras inglesas "*malicious*" e "*software*" representam grandes ameaças à Segurança Cibernética (HINTZBERGEN *et al.*, 2018).

Vecchia (2019) explica que um *malware* intenta contra a segurança das informações dos usuários e pode ser classificado em categorias.

Ainda segundo Vecchia (2019), um software malicioso tem a intenção de realizar atividades que prejudiquem a vítima, seja pela destruição de dados, corrupção do sistema, furto de informações, entre diversas outras. Dependendo das atividades realizadas pelo malware, ele é classificado em uma categoria (vírus, keylogger, backdoor, entre outros).

Dentre as categorias de softwares maliciosos se destacam alguns já identificados em ataques ao ambiente portuário, como é o caso dos *spywares* e *ransomwares*.

Hintzbergen *et al.* (2019) definem *spyware* como um programa que coleta informações no computador do usuário e as envia para outra parte. O *spyware* não tenta propositalmente danificar o dispositivo, mas sim, violar a privacidade. Velho (2016) destaca que os *spywares* são uma classe de *software* muito utilizada para obtenção de senhas de acesso.

Já o *ransomware*, segundo Vecchia (2019), trata-se de um *malware* que bloqueia o acesso a um dispositivo ou realiza a criptografia de arquivos. Para o desbloqueio/decifragem há a solicitação de um valor pecuniário à vítima.

Os vírus também integram o rol de ciberameaças naquele ambiente. Segundo Velho (2016), os vírus consistem em um software malicioso que se propaga realizando cópias de si mesmo ou infectando arquivos/programas presentes no computador. Necessitam ser explicitamente executados para iniciar suas atividades e infecção.

Os atacantes também podem explorar vulnerabilidades presentes nos dispositivos ou em seus softwares com objetivo de interromper atividades legítimas como sistemas *online*. Para Vecchia (2019), são chamados de ataques de negação de serviço.

A engenharia social é outra ferramenta utilizada pelos atacantes. Trata-se de técnicas de manipulação psicológica empregadas para persuadir a vítima e conduzi-la a execução de *malwares*, por exemplo. Contam com meios para despertar a curiosidade da vítima, abusar de sua ambição ou mesmo de sua inocência (VELHO, 2016).

Aliando técnicas de engenharia social, o *phishing* é outro tipo de ciberataque onde tipicamente a vítima recebe um e-mail, ou outra mensagem digital, e ao acreditar em seu conteúdo, atende aos comandos do atacante e repassa informações sensíveis como senhas e dados bancários (HINTZBERGEN *et al.*, 2018).

## 3 SEGURANÇA PORTUÁRIA

Há décadas que a segurança portuária figura entre o rol de assuntos de interesse do Governo brasileiro. Prova disso é o Decreto nº 1.507, de 30 de maio de 1995, que criou a Comissão Nacional e as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis, respectivamente Conportos e Cesportos.

A Conportos, por sua vez, elaborou e aprovou, em 02 de dezembro de 2002, o Plano Nacional de Segurança Pública Portuária, cujo teor visava a prevenção de ameaças à Segurança Pública encontradas nos portos, sendo elas relacionadas ao furto, roubo e contrabando de mercadorias, bem como ao tráfico de drogas e armas. As medidas constantes no PNSPP foram previstas com intenção de se auxiliar na redução da criminalidade no país (BRASIL, 2002).

Contudo, os atentados terroristas contra às torres do World Trade Center, ocorridos em 11 de setembro de 2001, trouxeram luz à importância da segurança dos portos e aeroportos a nível internacional. Neste sentido, a Organização Marítima Internacional acelerou a implementação do Código Internacional para Proteção de Navios e Instalações Portuárias – ISPS Code, que foi aprovado em 12 de dezembro de 2002 e passou a vigorar em 1° de julho de 2004. O referido código definiu novas medidas que visavam, inclusive, evitar a introdução e o trânsito de passageiros clandestinos e impedir ações terroristas e de sabotagem (BRASIL, 2020).

Nova regulamentação foi definida pela Conportos na busca do atendimento de todas as medidas contidas naquele Código, das quais merece destaque a necessidade de as instalações portuárias proverem avaliações de riscos inerentes à segurança que serviriam de base para a elaboração de seus respectivos Planos de Segurança.

Cabe ressaltar que os terminais portuários brasileiros são auditados pela Conportos e aqueles que cumprem as exigências do Código Internacional para Proteção de Navios e Instalações Portuárias são credenciados junto à Organização Marítima Internacional. A falta dessa credencial pode ser utilizada como justificativa para que os navios estrangeiros se recusem a atracar nos portos brasileiros. Podendo ainda, os portos internacionais, recusarem-se a receber os navios oriundos de portos descredenciados.

Um porto é um ambiente complexo e compreende ativos que são usados para fornecer uma variedade de serviços operacionais, onde a tecnologia desempenha um papel cada vez mais importante (BOYES; ISBELL; LUCK, 2020).

Em especial, a crise global ocasionada pelo COVID-19 impôs a necessidade de digitalização acelerada de diversos serviços, dentre eles, os portuários. A exemplo disso estão os sistemas de Janela Única, onde as agências reguladoras envolvidas podem ter acesso às informações das operações portuárias concentradas em um único sistema.

Neste sentido, diversos terminais portuários ao redor do mundo se viram diante de novas vulnerabilidades, sofrendo ataques através de seus sistemas de informação e comprometendo o cenário da segurança portuária.

## 3.1 CIBERATAQUES NO AMBIENTE PORTUÁRIO

Os principais portos marítimos sofreram uma média de 10 a 12 ciberataques por dia em 2017 (CEREMA, 2018). Os números tenderam ao crescimento, atingindo uma taxa de aumento de 400% no ano de 2020, sendo apontados os aumentos de *malwares*, *ransomwares* e *phising* (TME, 2020a).

Em 2013, o porto da Antuérpia descobriu que um cartel de drogas havia invadido seu sistema de gerenciamento de contêineres. De fato, a rede de computadores do porto era espionada desde junho de 2011, quando a rede teria sido infiltrada por *malware*, especificamente um *keylogger* (que permitia aos atacantes gravarem as teclas digitadas pelos operadores de carregamento/ descarregamento e, assim, obter nomes de usuário e senhas) (BATEMAN, 2013).

O porto de Roterdã foi infectado com uma versão modificada do *ransomware* NotPetya, o Petrwrap, em 2017. Em particular, terminais de contêineres operados pela APMT, uma subsidiária do grupo Moller-Maersk, viram suas atividades completamente paralisadas (REUTERS, 2017). Este mesmo ataque afetou o sistema da APM *Terminals* que opera dentro do porto de Itajaí, no estado de Santa Catarina, causando atrasos aos procedimentos do terminal (G1SC, 2017).

Um ano após o ataque ao porto de Roterdã, uma série de ataques cibernéticos interrompeu as atividades de vários portos internacionais. O porto de Long Beach, nos Estados Unidos da América, foi o primeiro a ser atingido, especificamente um terminal pertencente à China Ocean Shipping Company, que viu

seu sistema de informação contaminado pelo que parecia ser um *ransomware* (NERO, 2018).

O porto de Barcelona foi o próximo a ser atingido, ainda em 2018. Poucas informações foram repassadas ao público, mas parece que os sistemas internos de TI foram atacados, o que afetou os processos de carga/descarga (CYWARE, 2018).

Uma semana depois, o porto de San Diego também foi interrompido por um ataque cibernético. As autoridades portuárias confirmaram se tratar de um ataque *ransomware* que limitou severamente as capacidades de seus colaboradores, impactando no atendimento ao público (BBC, 2018).

No mesmo ano, o porto de Vancouver sofreu dois ataques de força bruta. Informações dão conta que 225 mil contas de usuários foram testadas até que se conseguisse o acesso aos sistemas (CIMPANU, 2018).

Em 2020, o porto de Marselha foi afetado incidentalmente devido ao ataque do *ransomware* Mespinoza/Pysa aos sistemas de informação da metrópole de Aix-Marseille-Provence (FILLIPPONE, 2020).

O porto iraniano de Shahid Rajaee, no mesmo ano, sofreu um ciberataque que afetou todos os seus computadores utilizados no serviço de regulação do fluxo de cargas, veículos e embarcações (WARRICK; NAKASHIMA, 2020).

O ataque ao porto de Kennewick bloqueou completamente o acesso aos seus servidores através de um *ransomware*. As consequências afetaram as instalações por aproximadamente uma semana (TME, 2020b).

No ano seguinte, 2021, quatros grandes portos da África do Sul – Cidade do Cabo, Ngqura, Elizabeth e Durban – foram paralisados após um ataque maciço à Autoridade Portuária Nacional da Transnet. O comunicado de imprensa oficial caracterizou o ataque com efeitos semelhantes ao de um *ransomware* (REUTERS, 2021).

No cenário nacional, se destaca o ataque ocorrido contra o porto de Mucuripe, em Fortaleza, no estado do Ceará. Como consequência, o terminal permaneceu com os sistemas comprometidos durante nove dias. Após a invasão ocorrida através de uma vulnerabilidade do sistema, os atacantes criptografaram as informações em troca de um resgate a ser pago pelo terminal (BRASILINE, 2019).

## 4 AÇÕES DE DEFESA

Em novembro de 2011, a Agência de Cibersegurançada da União Europeia lançava seu primeiro relatório sobre os desafios da cibersegurança no setor marítimo. No documento eram destacadas recomendações básicas para a segurança da informação nos terminais portuários, consideradas infraestruturas críticas para aquele bloco econômico. O relatório foi o passo inicial para novos estudos sobre o assunto, que culminaram, em dezembro de 2020, com a publicação das Diretrizes para o Gerenciamento de Riscos Cibernéticos nos Portos (DROUGKAS; SARRI; KYRANOUDI, 2020).

O Instituto de Engenharia e Tecnologia de Londres publicou em 2016 o Código de Práticas de Cibersegurança nos Portos e Sistemas Portuários. Revisada em 2020, a publicação tornou-se então o Guia de Boas Práticas de Cibersegurança nos Portos e Sistemas Portuários, que norteia as instalações portuárias do Reino Unido no que tange à segurança cibernética (BOYES; ISBELL; LUCK, 2020).

Recomendada pela própria Organização Marítima Internacional, as Diretrizes de Cibersegurança em Portos e Instalações Portuárias da Associação Internacional de Portos e Ancoradouros é a mais recente publicação sobre o assunto, envolvendo representantes de diversas autoridades portuárias internacionais e suas experiências adquiridas frente às dificuldades impostas pela pandemia COVID-19 (IAPH, 2021).

O atual regime nacional de segurança para a navegação e instalações portuárias, obedecendo às recomendações internacionais emanadas pela IMO, vem sendo atualizado com o propósito de fortalecer a segurança marítima e portuária, visando prevenir e prover resposta às ameaças. Em sua mais recente regulamentação - Resolução nº 53, de 04 de setembro de 2020[1] - a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis demonstra especial preocupação às ameaças relacionadas à Segurança da Informação, cujo tema deve ser abordado nas avaliações de risco e planos de segurança dos terminais, e dispõe de, pelo menos, 46 itens a serem verificados nos terminais para

[1] Resolução nº 53, de 04 de setembro de 2020. Disponível em: <Resolução nº 53, de 04 de setembro de 2020>. Acesso em: 10 nov. 2021.

que seja declarado o devido cumprimento do *ISPS Code*. Os itens baseiam-se na normativa ISO/IEC 27001 (BRASIL, 2020).

O principal porto marítimo da américa do norte em volume de contêineres e valor de carga, o porto de Los Angeles inaugurou neste ano seu Centro de Resiliência Cibernética (CRC). A solução visa melhorar a prontidão de segurança cibernética do porto e possibilitar o compartilhamento de indicadores de ameaças e possíveis medidas defensivas (CISO, 2022).

## 5 CONCLUSÃO

A digitalização e a automação do comércio marítimo e toda sua cadeia logística estão em andamento há muitas décadas em várias frentes. O cenário da pandemia do COVID-19 acelerou a tendência dos chamados "*smart ports"*.

Principais meios do comércio nacional e internacional, os portos também são grandes centros de troca de informações. O ritmo acelerado da digitalização dos portos e suas instalações intensifica a urgência de esforços voltados a medidas de resiliência cibernética, no sentido de proteger a integridade, disponibilidade e confidencialidade de dados críticos, proteger a infraestrutura marítima e garantir a prestação de serviços.

O setor marítimo em geral sofreu um aumento nos ataques cibernéticos, cujo risco tornou-se o principal para as autoridades e comunidade portuária. Importante ter em mente que os avanços tecnológicos, como inteligência artificial, aprendizado de máquina, internet das coisas e sistemas autônomos, trazem desenvolvimento ao setor portuário e marítimo ao mesmo tempo que oportunizam novas vulnerabilidades à cadeia global de suprimentos.

Os casos levantados nesse breve estudo apontam a iminência de maiores e mais constantes ataques ao setor portuário, sendo possível inferir que as consequências seriam de grandes proporções para toda cadeia logística nacional e até mesmo internacional.

As autoridades portuárias geralmente cedem as instalações portuárias à operadores de terminais privados com a pré-condição de que sejam gerenciadas e mantidas as infraestruturas necessárias às operações. Àquelas, portanto, resta assumir a responsabilidade natural de coordenação entre os atores da comunidade portuária e adotar medidas que padronizem e unifiquem a cultura de segurança da informação no ambiente portuário. Em especial, no Brasil, deve-se tomar consciência da atual importância da segurança da informação no contexto da segurança portuária. As agências governamentais devem ser cooptadas a participar na internalização de diretrizes já estabelecidas internacionalmente, tratando os portos e instalações portuárias como infraestruturas críticas e de suma importância para o desenvolvimento econômico nacional.

## REFERÊNCIAS


BATEMAN, T. **Police warning after drug traffickers' cyber-attack.** BBC News, publicado em: 16 out. 2013. Disponível em: <https://www.bbc.com/news/world-europe-24539417>. Acesso em: 13 nov. 2021.

BRASIL. **Plano nacional de segurança pública portuária.** Ministério da Justiça e Segurança Pública, publicado em: 02 dez. 2002. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/seguranca-portuaria/planonacionalPNSPPjustiapontogov.pdf>. Acesso em: 13 nov. 2021.

BRASIL. **Segurança portuária.** Ministério da Justiça e Segurança Pública, publicado em: 19 de jun. de 2020. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/seguranca-portuaria>. Acesso em: 15 nov. 2021.

BBC. **San Diego port hit by ransomware attack.** Copyright© BBC News, publicado em: 28 set. 2018. Disponível em: <https://www.bbc.com/news/technology-45677511>. Acesso em: 13 nov. 2021.

BOYES, H.; ISBELL, R.; LUCK, A. **Good practice guide cyber security for ports and port systems.** Londres: Institution of Engeneering and Technology, 2020.

BRASILINE. **Porto de Fortaleza completa uma semana refém de ciberataque.** Copyright© Brasiline Tecnologia, publicado em: 6 nov. 2019. Disponível em: <https://brasiline.com.br/blog/porto-de-fortaleza-completa-uma-semana-refem-de-ciberataque/>. Acesso em: 13 nov. 2021.

CEREMA. **Assises port du futur 2017.** CEREMA, publicado em: 29 jul. 2018. Disponível em: <https://www.portdufutur.fr/sites/portdufutur/files/fichiers/2019/02/weblight%20Essentiel%20Port%20du%20futur%202017-29-06-18.pdf>. Acesso em: 13 nov. 2021.

CIMPANU, C. **Cyber-attaque: les ports de Barcelone et San Diego pris pour cible.** Copyright© ZDNET, A RED VENTURES COMPANY, publicado em: 28 set. 2018. Disponível em: <https://www.zdnet.fr/actualites/cyber-attaque-les-ports-de-barcelone-et-san-diego-pris-pour-cible-39874329.htm>. Acesso em: 13 nov. 2021.

CISO. **Porto de Los Angeles abre centro de ciber-resiliência.** Da redação da Ciso advisor, publicado em: 25 jan. 2022. Disponível em: <https://www.cisoadvisor.com.br/porto-de-los-angeles-abre-centro-de-ciber-resiliencia/>. Acesso em: 13 jan. 2022.

CYWARE. **Porto of Barcelona suffers a cyberattack that impacted many of its servers.** Copyright© Cyware Social, publicado em: 24 set. 2018. Disponível em: <https://cyware.com/news/port-of-barcelona-suffers-a-cyberattack-that-impacted-many-of-its-servers-5f22c204>. Acesso em: 13 nov. 2021.

DROUGKAS, A.; SARRI, A.; KYRANOUDI, P. **Cyber risk management for ports:** guidelines for cybersecurity in the maritime sector. European Union Agency for Cybersecurity. 2020.

FILLIPPONE, D. **Aix-Marseille-Provence touchée par une cyberattaque. Copyright© LeMondeInformatique.fr**, publicado em: 16 mar. 2020. Disponível em: <https://www.lemondeinformatique.fr/actualites/lire-aix-marseille-provence-touchee-par-une-cyberattaque-78444.html>. Acesso em: 13 nov. 2021.

G1SC. **Ciberataque mundial afeta operação no porto de Itajaí.** Portal G1 SC, publicado em: 29 jun. 2017. Disponível em: <https://g1.globo.com/sc/santa-catarina/noticia/ciberataque-mundial-afeta-operacao-no-porto-de-itajai.ghtml>. Acesso em: 13 nov. 2021.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, HANS. **Fundamentos de segurança da informação:** Com base na ISO 27001 e na ISO 27002. 3. ed. Rio de Janeiro: Brasport, 2018.

IAPH. **IAPH Cybersecurity guidelines for ports and port facilities.** International Association of Ports and Harbors (IAPY), publicado em: 02 jul. de 2021. Disponível em: <https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf>. Acesso em: 10 nov. 2021.

MILLER, L.C. **Cybersecurity for dummies.** 2. ed. New Jersey: Palo Alto Networks, 2016.

NERO, M. E. **Long Beach port terminal hit by ransomware attack.** Press-telegram, publicado em: 24 jul. 2018. Disponível em: <https://www.presstelegram.com/2018/07/24/ long-beach-port-terminal-hit-by-ransomware-attack/>. Acesso em: 13 nov. 2021.

REUTERS. **Cyberattack hits 17 APM shipping container terminals: Dutch broadcaster RTV.** Publicado pelo Reuters Staf em: 27 jun. 2017. Disponível em: <https://www.reuters.com/article/us-cyber-attack-maersk-apm-idUSKBN19I1X3>. Acesso em: 13 nov. 2021.

REUTERS. **South Africa's transnet restores operations at ports after cyber attack.** Publicado pelo Reuters Staf em: 29 jul. 2021. Disponível em: <https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ>. Acesso em: 13 nov. 2021.

TME. **Report: Maritime cyberattacks up by 400 percent.** Copyright© The Maritime Executive, LLC. Publicado em: 04 jun. 2020a. Disponível em: <https://www.maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent>. Acesso em: 13 nov. 2021.

TME. **Ransomware cripples IT systems of inland port in Washington State.** The maritime executive, 19 nov. 2020b. Disponível em: <https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state>. Acesso em: 13 nov. 2021.

VECCHIA, E. D. **Perícia digital:** Da investigação à análise forense. 2. ed. Campinas: Millenium editora, 2019.

VELHO, J. A. **Tratado de computação forense.** Campinas: Millenium editora: 2016.

WARRICK, J.; NAKASHIMA, E. **Officials: Israel linked to a disruptive cyberattack on Iranian port facility.** The Washington Post, publicado em: 18 mai. 2020. Disponível em: <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html>. Acesso em: 13 nov. 2021.