Anais do Congresso Brasileiro de Iniciação Científica
(https://periodicos.unisanta.br/COB)

ISSN 2317-1316

CIBERSEGURANÇA NO TRANSPORTE MARÍTIMO: A INFLUÊNCIA DAS MEDIDAS DA INTERNATIONAL MARITIME ORGANIZATION (IMO) NO CIBERATAQUE À MEDITERRANEAN SHIPPING COMPANY (MSC) EM ABRIL DE 2020

CYBERSECURITY IN MARITIME TRANSPORTATION: THE INFLUENCE OF INTERNATIONAL MARITIME ORGANIZATION (IMO) MEASURES ON THE APRIL 2020 CYBERATTACK AGAINST MEDITERRANEAN SHIPPING COMPANY (MSC)

Thamyris Gomes de Jesus, Igor Alves da Silva, Kelvin do Nascimento Silva, Paloma Ramos de Lima, Giovanna Marcely Oliveira da Silva, Luiz André Silva Evangelista

Universidade Santa Cecília, Curso de Relações Internacionais
E-mail para contato: kelvinsilvaofficial5@gmail.com

RESUMO – A empresa Mediterranean Shipping Company (MSC) sofreu um ataque de malware em abril de 2020, demonstrando que a digitalização do transporte marítimo, embora tenha proporcionado maior eficiência a operações, também ampliou os riscos relacionados à cibersegurança. Nesse contexto, o presente trabalho busca analisar e compreender como a Organização Marítima Internacional (IMO) e a multinacional Mediterranean Shipping Company (MSC) se comportam e agem diante das ameaças contemporâneas no centro cibernético do setor marítimo.

Palavras-chave: Cibersegurança; IMO; MSC; Malware; Segurança marítima.

ABSTRACT – The Mediterranean Shipping Company (MSC) suffered a malware attack in April 2020, demonstrating that the digitalization of maritime transportation, although it has provided greater efficiency to operations, has also increased cybersecurity-related risks. In this context, this study aims to analyze and understand how the International Maritime Organization (IMO) and the multinational Mediterranean Shipping Company (MSC) behave and act in response to contemporary threats in the cybersecurity sector of the maritime industry.

Keywords: Cybersecurity; IMO; MSC; Malware; Maritime transport.

ISSN 2317-1316

1 INTRODUÇÃO

Em razão do expressivo aumento da digitalização do setor marítimo, diversos processos operacionais e informacionais começaram a serem automatizados. Todavia, essa crescente automatização e digitalização também colocou as organizações a maiores exposições no espaço digital, expondo-as a ataques cibernéticos e promovendo cada vez mais os debates para as criações de mecanismos de segurança digital.

Devido aos fatos expostos, a cibersegurança passou a se tornar um fator de posição estratégica nos setores de gestão de riscos das empresas, visando maior proteção dos sistemas de comunicação e tecnológicos da mesma. Ademais, a International Maritime Organization (IMO) tem auxiliado grandes companhias empresariais com o desenvolvimento de diretrizes que identifiquem, previnam e gerenciem riscos de ataques cibernéticos.

Um caso de alta relevância de ataque cibernético no setor marítimo foi contra a Mediterranean Shipping Company (MSC) em abril de 2020, cuja sofreu um ataque de *malware*[1] direcionado a sua sede em Genebra, afetando todas as operações e gerando indisponibilidade temporária em seus serviços. Esse ataque cibernético evidenciou as fragilidades de grandes empresas do referido setor e reforçou o delineamento de estratégias para a segurança digital no âmbito do escopo marítimo.

Por fim, destaca-se que o estudo se baseia em analisar os mecanismos e medidas de cibersegurança aplicadas ao transporte marítimo, tendo como base as orientações da IMO e consequências que advieram do ataque contra a MSC e como objetivo compreender as fragilidades e meios de como prevenir e gerir riscos futuros relacionados à segurança digital contra ataques cibernéticos no âmbito do transporte marítimo.

2 MATERIAIS E MÉTODOS

Este artigo adota uma abordagem qualitativa de cunho exploratório e analítico com base em revisões bibliográficas e documentais. A pesquisa examina medidas e mecanismos voltados a cibersegurança aplicados no transporte marítimo pela International Maritime Organization (IMO), sendo a agência especializada da Organização das Nações Unidas

[1] Malware é qualquer programa de computador ou software que seja projetado para fins maliciosos. O malware é utilizado para roubar dados ou causar danos em computadores ou sistemas de software.

ISSN 2317-1316

(ONU) responsável por regular a segurança, a proteção e o desempenho ambiental do transporte marítimo internacional.

A coleta de dados foi realizada por meio de fontes primárias e secundárias. Entre as fontes primárias, destacam-se documentos e diretrizes oficiais da IMO relacionados ao gerenciamento de riscos cibernéticos marítimos, especialmente as *Guidelines on Maritime Cyber Risk Management* e a Resolução MSC.428(98), além de informações oficiais divulgadas pela própria MSC sobre o incidente ocorrido em abril de 2020. Como fontes secundárias, foram utilizados artigos acadêmicos e publicações especializadas sobre cibersegurança, transporte marítimo e riscos associados à digitalização do setor. A análise de conteúdo foi empregada para identificar as principais vulnerabilidades, medidas de proteção, impactos operacionais e mecanismos de resposta relacionados ao caso da MSC.

Nesse sentido, a escolha do caso justifica-se pela relevância do incidente que a MSC sofreu um ataque de *malware* que afetou sistemas de sua sede em Genebra, ocasionando a indisponibilidade temporária de ferramentas digitais e de seu website. a fim de identificar, empiricamente, os desafios enfrentados pelo setor marítimo diante da crescente dependência de sistemas digitais e avaliar a importância das medidas de gerenciamento de riscos cibernéticos promovidas pela IMO.

3 RESULTADOS E DISCUSSÃO

Em abril de 2020, a Mediterranean Shipping Company (MSC) sofreu um ataque cibernético que afetou parte de sua infraestrutura digital na sede localizada em Genebra, na Suíça. O incidente inicialmente foi identificado como uma indisponibilidade de rede e levou a empresa a retirar determinados sistemas de funcionamento como medida preventiva, enquanto sua equipe de tecnologia da informação investigava a origem do problema. Após a realização de uma investigação, a MSC confirmou que se tratava de um ataque de *malware* baseado em uma vulnerabilidade direcionada. O incidente afetou o centro de dados da empresa, seu website e algumas de suas ferramentas digitais, incluindo o sistema myMSC, utilizado para serviços relacionados às operações de transporte de cargas (MSC, 2020).

A indisponibilidade dos sistemas ocorreu durante o feriado de Páscoa e permaneceu por alguns dias, sendo os principais serviços digitais restabelecidos em 15 de abril de 2020.

ISSN 2317-1316

Apesar do ocorrido, a MSC informou que o incidente permaneceu restrito aos sistemas localizados em sua sede em Genebra e não provocou a paralisação de suas demais operações. Agências, terminais, depósitos e outros departamentos da companhia continuaram funcionando, permitindo a manutenção do fluxo de cargas durante o período. Além disso, foram disponibilizados meios alternativos para que os clientes realizassem reservas e acompanhassem suas operações, incluindo contato por telefone, e-mail e plataformas digitais de terceiros. Outro aspecto relevante do incidente refere-se aos seus efeitos sobre a segurança das informações. Após a investigação, a MSC declarou não ter identificado, até aquele momento, perda ou comprometimento de dados decorrente do ataque (MSC, 2020).

O caso evidenciou que, a indisponibilidade temporária de sistemas utilizados para reservas, acompanhamento de cargas e comunicação com clientes demonstra que os impactos de um incidente cibernético podem ocorrer mesmo quando não há evidências de vazamento ou destruição de dados. Nesse sentido, o caso da MSC evidencia que a cibersegurança no transporte marítimo envolve também a disponibilidade e a continuidade dos sistemas necessários ao funcionamento das atividades logísticas (MSC, 2020; KUHN et al., 2021).

O episódio também demonstra uma característica importante dos riscos cibernéticos no setor marítimo: a crescente dependência de sistemas digitais cria novas possibilidades de eficiência, mas simultaneamente amplia os pontos que podem ser explorados por ameaças cibernéticas. Estudos sobre a digitalização do transporte marítimo identificam o ataque sofrido pela MSC em 2020 como um dos incidentes relevantes do período, destacando que o malware provocou uma interrupção dos sistemas da companhia em sua sede de Genebra, embora os danos operacionais tenham sido limitados quando comparados a outros ataques registrados no setor (KUHN et al., 2021).

A partir do caso da MSC, torna-se possível analisar a cibersegurança marítima não apenas como uma questão relacionada à proteção de informações, mas também como um componente da continuidade e da resiliência das operações. A capacidade da empresa de restringir o incidente à sua sede, manter suas operações globais em funcionamento e disponibilizar canais alternativos de atendimento demonstra a importância dos mecanismos de resposta e recuperação diante de ameaças cibernéticas. Essa perspectiva se relaciona

ISSN 2317-1316

diretamente às diretrizes desenvolvidas pela Organização Marítima Internacional (IMO), que passaram a incorporar o gerenciamento dos riscos cibernéticos aos sistemas de gestão de segurança do transporte marítimo (IMO, 2026).

Nas Organizações Internacionais, a Organização Marítima Internacional (IMO) desempenha um papel fundamental na padronização da segurança operacional de transportes marítimos. Conforme aumento crescente da digitalização e cada vez mais riscos de vulnerabilidade a incidentes e ataques de cibersegurança, a IMO implementou a integração de seus gerenciamentos de riscos cibernéticos aos sistemas de gestão de segurança corporativa de empresas de navegação marítima (IMO, 2026).

As diretrizes da IMO estabelecem que a cibersegurança deve ser parte intrínseca do funcionamento operacional e da segurança da navegação marítimas. Nesse sentido, destacam-se aspectos na estrutura de suas diretrizes como a Inclusão no Código ISM (*International Safety Management*). Conforme Resolução MSC.428(98), a IMO determinou que os Sistemas de Gestão de Segurança das empresas marítimas devem possuir adequadamente os riscos cibernéticos, tornando tal avaliação obrigatória em auditorias e verificações de conformidade. As diretrizes da organização formam base para a gestão de riscos cibernéticos em cinco funções fundamentais, alinhadas a *frameworks* internacionais de segurança. Identificando através de mapeamento de ativos, sistemas de Tecnologia da Informação (TI) e de Tecnologia Operacional (TO).

Implementando proteção através de medidas de controle de acesso, barreiras técnicas e salvaguardas para minimizar a probabilidade de falhas e invasões. No caso observado, a MSC sofreu incidentes cibernéticos em diferentes momentos, medidas como segmentação de redes e controles de acesso são exemplos de mecanismos para impedir que um ataque comprometa toda a infraestrutura. Desenvolvendo mecanismos de monitoramento contínuo para a identificar de maneira eficaz falhas e incidentes cibernéticos. Formulando planos de ação aos riscos e procedimentos operacionais, contendo os impactos e minimizando incidentes. Estabelecendo estratégias de restauração de dados, sistemas e infraestruturas críticas, garantindo a continuidade dos negócios em mediante crises.

A segunda função está relacionada à proteção com medidas de controle de acesso, entre elas: barreiras técnicas e salvaguardas para minimizar a probabilidade de falhas e invasões. No caso da MSC, após a identificação inicial do problema, determinados sistemas

ISSN 2317-1316

foram retirados de funcionamento como medida preventiva enquanto a equipe de tecnologia da informação investigava a origem do incidente. Essa medida contribuiu para controlar o risco aos sistemas localizados na sede em Genebra e evitar que o problema afetasse suas demais operações (MSC, 2020).

A terceira função está relacionada à detecção, monitorando contínuo para identificar de maneira eficaz falhas e incidentes cibernéticos. No caso da MSC, a detecção da indisponibilidade de rede e a investigação realizada, permitiram reconhecer que o problema não se tratava apenas de uma falha operacional, mas de um ataque de *malware*. Dessa forma, a empresa conseguiu identificar rapidamente a origem do incidente e avaliar os sistemas que haviam sido afetados (MSC, 2020).

A quarta função está relacionada à resposta, formulando planos de ação aos riscos e procedimentos operacionais, contendo os impactos e minimizando incidentes. Durante o ataque, a MSC retirou determinados sistemas de funcionamento e disponibilizou meios alternativos para que os clientes realizassem reservas e acompanhassem suas operações, incluindo contato por telefone, e-mail e plataformas digitais de terceiros. Além disso, agências, terminais, entre outros departamentos da companhia continuaram funcionando, permitindo a manutenção do fluxo de cargas durante o período em que seus sistemas estavam indisponíveis (MSC, 2020).

A quinta função está relacionada à recuperação, estabelecendo estratégias de restauração de dados, sistemas e infraestruturas críticas, garantindo a continuidade dos negócios mediante crises. No caso observado, os principais serviços digitais foram restabelecidos em 15 de abril de 2020, após permanecerem indisponíveis por alguns dias. A manutenção das demais operações e a disponibilização de canais alternativos demonstram a importância da recuperação e da continuidade das atividades diante de um incidente cibernético (MSC, 2020).

ISSN 2317-1316

Quadro 1 - Medidas da International Maritime Organization para o gerenciamento de riscos cibernéticos marítimos:

Medida da IMO	Objetivo	Relação com o caso MSC
MSC-FAL.1/Circ.3/Rev.3 – Guidelines on Maritime Cyber Risk Management	Busca proteger, identificar e responder a incidentes cibernéticos. Também identifica formas de autoproteção contra ataques.	Reduz vulnerabilidades diminuindo possíveis impactos nas operações da MSC.
Resolução MSC.428(98)	Integrar o gerenciamento de riscos cibernéticos aos *Safety Management Systems* (SMS).	Estabelece que o risco cibernético seja incorporado à gestão de segurança da companhia.
Identificação e proteção de sistemas críticos	Reconhecer ativos vulneráveis e implementar medidas de proteção e continuidade.	Pode reduzir a possibilidade de comprometimento de sistemas essenciais à operação da empresa.
Detecção, resposta e recuperação	Estabelecer mecanismos para identificar incidentes, responder a eles e restaurar sistemas afetados.	Pode reduzir a duração e a extensão dos impactos decorrentes de um ataque.

Fonte: Elaborado pelos autores com base em documentos oficiais da IMO (2025).

4 CONCLUSÃO

Com base nos estudos avaliados no artigo, identifica-se que a cibersergurança é fundamental para garantir a segurança, a continuidade e a resiliência nas operações marítimas. Embora a MSC não tenha sido prejudicada em suas operações, ainda assim, sua falha fica evidente e a segurança em suas operações também, demonstrando que a segurança absoluta no âmbito cibernético é impraticável, até mesmo para multinacionais de grande porte.

As empresas devem estar preparadas para prevenir, identificar e responder rapidamente a incidentes cibernéticos. Nesse contexto, as diretrizes da IMO, contribuem para fortalecer o gerenciamento desses riscos e reduzir os impactos de possíveis ataques, fazendo da cibersegurança uma parte essencial da gestão e segurança do transporte marítimo.

ISSN 2317-1316

5 DECLARAÇÃO DE USO DE IA

Durante a elaboração deste trabalho, utilizou-se a ferramenta ChatGPT para organizações de tópicos centrais da pesquisa e revisões de coesão e coerência do texto. O conteúdo gerado foi revisado, editado e validado pela autora, que assume total responsabilidade pelo texto final.

6 REFERÊNCIAS

FORTINET. **O que é malware? Como prevenir ataques de malware?** [S. l.]: Fortinet, [s. d.]. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/malware. Acesso em: 9 set. 2026.

INTERNATIONAL MARITIME ORGANIZATION (IMO)**.** ***Guidelines on maritime cyber risk management*****.** MSC-FAL.1/Circ.3/Rev.3. London: IMO, 2025.

INTERNATIONAL MARITIME ORGANIZATION (IMO). ***Maritime cyber risk management in safety management systems*****.** Resolution MSC.428(98). London: IMO, 2017

INTERNATIONAL MARITIME ORGANIZATION (IMO). **Maritime cyber risk**. London: IMO, 2026. Disponível em: https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx. Acesso em: 6 out. 2026.

KUHN, Kristen; BICAKCI, Salih; SHAIKH, Siraj Ahmed. **COVID-19 digitization in maritime: understanding cyber risks**. *WMU Journal of Maritime Affairs*, v. 20, n. 2, p. 193-214, 2021.

MEDITERRANEAN SHIPPING COMPANY (MSC). **Network outage resolved.** 15 abr. 2020. Disponível em: https://www.msc.com/en/newsroom/news/2020/april/network-outage-resolved. Acesso em: 6 out. 2026.