10928074 08020.000896/2020-52

Ministério da Justiça e Segurança Pública
Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis - Conportos

OFÍCIO-CIRCULAR Nº 1/2020/CONPORTOS/MJ

Brasília, 02 de março de 2020.

Aos Senhores
Coordenadores de Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Cesportos)
Representantes legais de Organizações de Segurança (OS)

Assunto: **Risco Cibernético - Estudo de Avaliação de Risco**

Senhores Coordenadores,

1. Em março de 2019, a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Conportos) instituiu um grupo de trabalho com o propósito de internalizar em suas normas a aplicação de diretrizes de uma metodologia de análise de riscos voltada especialmente para instalações portuárias, adotando-se como referência o trabalho acadêmico Análise de Riscos com Ênfase em Segurança Portuária (ARESP) - vide https://periodicos.pf.gov.br/index.php/RBCP/article/view/580 .

2. É importante destacar que a ARESP encontra abrigo no Código ISPS, já devidamente internalizado na legislação brasileira pelo Decreto nº 9.988, de 26 de agosto de 2019, o qual determina a realização de uma "*Avaliação de Proteção*" com a identificação dos ativos de interesse da instalação portuária, suas vulnerabilidades, as possíveis ameaças, bem como as consequências de eventuais ações adversas.

3. No decorrer dos trabalhos do grupo, ao se estudar as possíveis ameaças, foram registradas as ocorrências de ataques cibernéticos em dois portos organizados (Natal/RN e Fortaleza/CE), onde ocorreram sequestros de dados, impactando as atividades desses portos, em situações que se configuram como incidentes de proteção, conforme definido no Decreto nº 6.869, de 4 de junho de 2009.

4. Em face dos ataques cibernéticos assinalados e dos estudos que apontam para o crescimento de incidentes nessa área, a Conportos tem adotado uma postura mais rigorosa na análise dos Estudos de Avaliação de Risco e Planos de Segurança Portuária pela perspetiva da abordagem dos riscos cibernéticos.

5. Enquanto algumas Organizações de Segurança já incorporaram essa necessidade em seus trabalhos, identificando riscos cibernéticos e propondo a adoção de medidas de proteção minimamente adequadas, em consultas encaminhadas à Secretaria-Executiva da Conportos, alguns interlocutores têm apresentado objeções à abordagem dos riscos cibernéticos nos Estudos de Avaliação de Risco e Planos de Segurança Portuária, alegando tratar-se de assunto eminentemente técnico e que as instalações portuárias, normalmente, já cumprem uma série de medidas impostas por seus controladores, não permitindo acesso às informações necessárias para uma análise de riscos.

6. Convém registrar que a parte "B" do Código ISPS contém as instruções para a elaboração dessa Avaliação de Proteção, listando que o documento final deve cobrir os seguintes elementos dentro das instalações portuárias (subitem 15.3):

a) proteção física;

b) integridade estrutural;

c) sistemas de proteção de pessoal;

d) programas de procedimentos;

e) sistemas de rádio e de telecomunicações, **incluindo sistemas e redes de informática**;

f) infraestrutura de transporte relevante;

g) utilidades públicas; e

h) outros elementos que possam, caso danificados ou utilizados para observação ilícita, apresentar um risco a pessoas, propriedade ou operações dentro da instalação portuária.

7. O subitem 15.7 da parte "B" do Código ISPS, por sua vez, define os bens móveis e infraestrutura (ativos) que devem ser considerados como importantes para proteger:

a) áreas de acesso, entradas, aproximações, ancoragem, manobras e atracação;

b) instalações de cargas, terminais, áreas de armazenagem e equipamentos para manuseio de cargas;

c) sistemas, tais como sistemas de distribuição elétrica, sistemas de rádio e telecomunicações e **sistemas e redes de informática**;

d) sistemas de gestão de tráfego de navios no porto e sistemas de auxílio à navegação;

e) instalação de energia, tubulação de transferência de cargas e abastecimento de água;

f) pontes, ferrovias e estradas;

g) embarcações de serviços portuários, incluindo embarcações de praticagem, rebocadores, chatas, *etc* ;

h) sistemas e equipamentos de proteção e vigilância; e

i) águas adjacentes às instalações portuárias.

8. E, por fim, o subitem 15.11 do normativo prescreve que a Avaliação de Proteção deve considerar todas as possíveis ameaças, a seguir listando alguns exemplos de incidentes de proteção a serem considerados.

9. Diante desse cenário, a Conportos entende que os ataques cibernéticos devem ser incluídos na lista de ameaças a considerar, mesmo não estando literalmente expressos nos subitens em comento.

10. Após constatar o risco crescente no contexto portuário nacional e demonstrar a necessidade de abordagem dos sistemas e redes de informática no âmbito de uma Avaliação de Proteção regida pelo Código ISPS, o grupo de trabalho instituído pela Conportos está elaborando uma ferramenta que auxiliará na identificação e valoração de vulnerabilidades, ameaças e consequências em todas as áreas de uma instalação portuária, incluindo a área de Tecnologia da Informação (TI).

11. Enquanto esse trabalho não for finalizado, recomenda-se que as Organizações de Segurança e as Unidades de Segurança Organizacionais passem a tratar do tema em pauta na elaboração dos Estudos de Avaliação de Risco e Planos de Segurança Portuária, adotando uma abordagem mais detalhada e abrangente.

12. Os documentos devem estabelecer uma política de segurança contemplando expressamente as medidas de proteção a serem aplicadas aos usuários, ambientes físico e lógico de seus sistemas, processos e aspectos tecnológicos da instalação portuária.

13. É preciso explicitar as regras de segurança para o acesso físico e lógico às informações armazenadas em seus sistemas de computação, considerando ameaças, externas e internas, como por exemplo: I) ligações de pontos de rede clandestinos; II) acessos indevidos a informações; III) uso de softwares não autorizados; IV) contaminação de computadores e sistemas por vírus; V) furtos de dispositivos; VI) acessos não autorizados, físico e/ou lógico; VII) congestionamento do sistema causado por tentativas de acesso em grande quantidade; VIII) *Ransomware.*

14. É fundamental que os Estudos de Avaliação de Risco e Planos de Segurança Portuária abordem claramente as regras de identificação e utilização de seus usuários, os procedimentos de resguardo de suas plantas lógica e física, a prevenção a acessos indevidos às estações de trabalho e equipamentos críticos de suas redes, a utilização de antivírus atualizados, as rotinas de *backup etc*.

15. Para subsidiar os trabalhos das Organizações de Segurança e as Unidades de Segurança Organizacionais, a Conportos sugere a leitura dos seguintes trabalhos:

a) http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20(E).pdf ;

b) https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport ;

c) http://portalcip.org/wp-content/uploads/2019/08/C05-Cyber-Security-Assessment.pdf ;

d) Normas ISO/IEC da série 27000, com ênfase na norma ISO/IEC 27005 (*Information Security Risk Management*) ;

e) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf .

16. Sublinhe-se que, como demonstrado, a abordagem dos riscos cibernéticos não é um item opcional, estando no escopo dos trabalhos previstos pelo Código ISPS e, consequentemente, pelos normativos da Conportos, sobretudo quando o objetivo é, no caso de um incidente de proteção, que a instalação portuária continue a operar sem interrupção ou comprometimento dos serviços prestados aos seus usuários (resiliência).

17. Vale dizer, as instalações portuárias que deixarem de observar na elaboração dos Estudos de Avaliação de Risco e Planos de Segurança Portuária as boas práticas de segurança cibernética, dificultando ou negando acesso às informações necessárias para o regular desenvolvimento da gestão de risco pelas respectivas Organizações de Segurança ou Unidades de Segurança Organizacionais, não terão seus documentos homologados pela Conportos.

18. Por fim, no tocante a eventuais alegações de dificuldades para o trato do tema, por parte das Organizações de Segurança e Unidades de Segurança Organizacionais, devido ao seu caráter estritamente técnico, impende ressaltar que o Código ISPS prevê expressamente que as pessoas envolvidas em uma Avaliação de Proteção devem poder recorrer à assistência de especialistas, conforme disposto no subitem 15.4 da parte "B".

19. **Ante o exposto, a Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Conportos) dá ciência a todas as Organizações de Segurança, a fim de que incorporem os riscos cibernéticos em seus procedimentos de elaboração de Estudos de Avaliação de Risco e Planos de Segurança Portuária, bem como a todas as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Cesportos) para que orientem as instalações portuárias com Unidades de Segurança Organizacionais credenciadas em suas respectivas circunscrições e observem as prescrições apresentadas.**

Atenciosamente,

MARCELO JOÃO DA SILVA
Delegado de Polícia Federal
Presidente da Conportos

Documento assinado eletronicamente por **MARCELO JOÃO DA SILVA**, **Presidente da CONPORTOS**, em 05/03/2020, às 17:58, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **10928074** e o código CRC **B69AC0F8**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 08020.000896/2020-52 SEI nº 10928074

Setor de Autarquias Sul - SAS - Quadra 06 - Lotes 9/10, Edifício Sede da Polícia Federal - 6º andar - salas 641/642 - Bairro Setor de Autarquias Sul, Brasília/DF, CEP 70037-900
Telefone: (61) 2024-8750/8058/7901/8649 - https://www.justica.gov.br
Para responder, acesse https://sei.protocolo.mj.gov.br