RESUMO

O estudo teve por objetivo geral estabelecer diretrizes de uma metodologia de análise de riscos com ênfase em instalações portuárias. A padronização de procedimentos a serem realizados nos portos brasileiros em cumprimento ao previsto no *ISPS Code* e nas Resoluções da CONPORTOS é elemento fundamental para a consolidação do Plano de Segurança Portuária. Dessa forma, a iniciativa deste trabalho vem no sentido de formalizar um processo de análise de riscos com vistas a possibilitar a sua sedimentação entre os entes envolvidos nesse processo: trata-se da Análise de Riscos com Ênfase em Segurança Portuária (ARESP).

Palavras-chave: Estudo de Avaliação de Riscos. Plano de Segurança Portuária. ISPS Code. CONPORTOS.

ABSTRACT

The general objective of the paper was to establish guidelines for a risk analysis methodology with emphasis on port facilities. The standardization of procedures to be accomplished in Brazilian ports in compliance with the provisions of the ISPS Code and the CONPORTOS Resolutions is a fundamental element for the consolidation of the Port Security Plan. Thus, the initiative of this work is to formalize a process of risk analysis with the objective to enabling its settlement among the entities involved in this process: this is the Risk Analysis with Port Security Emphasis (ARESP).

Keywords: Risk Assessment Analysis. Port Security Plan. ISPS Code. CONPORTOS.

ANÁLISE DE RISCOS COM ÊNFASE NA SEGURANÇA PORTUÁRIA: O PROCESSO DE AVALIAÇÃO DE RISCOS DA CONPORTOS E O ISPS CODE

Felipe Scarpelli

1. Introdução

O transporte fluvial e marítimo têm como característica um custo operacional mais baixo ao associar grande capacidade de carga e pouco consumo de energia, mostrando-se como o melhor meio de transporte para grandes distâncias se comparado ao modais aéreo ou terrestre.

No Brasil, os portos exercem um papel fundamental e estratégico na medida em que constituem uma das principais infraestruturas de apoio ao comércio exterior – atualmente, cerca de 95% das mercadorias exportadas/importadas pelo Brasil passam por terminais portuários. Apresentam-se como o elo da troca de modais na cadeia logística de transporte e viabilizam boa parte do modelo economico por meio da aplicação de sua política tributária, ou seja, trata-se de um ponto de confluência das riquezas a serem transferidas entre nações produtoras e consumidoras.

Devido à sua importância econômica e ao grande desafio em se proteger as instalações e as áreas aquáticas, os portos são alvos reais ou potenciais de ações criminosas, movimentos sociais, atos terroristas etc.

Nesse sentido, ao se analisar a relevância e o contexto nos quais os terminais portuários estão inseridos, onde há grande volume de informações difusas e distintas ameaças como o terrorismo marítimo, pirataria, organizações criminosas, movimentos sociais, entre outras, percebe-se, cada vez mais, a necessidade de se definir estratégias que garantam a diminuição das vulnerabilidades portuárias balizadas em conhecimento técnico.

Não obstante, surgiram novas exigências no contexto mundial de forma a elevar os níveis de segurança para a atividade, estabelecendo parâmetros de proteção para os navios e para as instalações portuárias.

A *International Maritime Organization* (IMO), elaborou a Circular nº 443 do Maritime Safety Committee[1], de 26 de setembro de 1986, recomendando aos países menbros da Organização das Nações Unidas (ONU) a adoção de diversas medidas protetivas, como a criação de Planos de Segurnaça nos Portos; Planos de Segurança para Navios; criação de áreas restritas, barreiras, instalação de alarmes e sistemas de comunicações e controles de acesso e identificação, entre outras.

Ainda, após o ataque às torres gêmeas nos Estados Unidos, em 11 de setembro de 2001, a IMO recomendou novas medidas de proteção a navios e instalações portuárias. Com efeito, em 12 de dezembro de 2002, foi implementado o *International Ship and Port Facility Security Code*[2] (ISPS Code), onde apresenta como um de seus objetivos o de prover uma metodologia para avaliações de segurança de modo a desenvolver planos e procedimentos a fim de responder às ameaças reais ou potenciais que podem impactar a atividade portuária – trata-se do Estudo de Avaliação de Riscos (EAR), objeto deste estudo.

No Brasil, a implantação do *ISPS Code* dividiu-se da seguinte forma: (I) - À Marinha do Brasil coube a responsabilidade pela implantação do Código no que diz respeito aos navios e plataformas móveis de perfuração situadas ao longo da costa brasileira; (II) – À Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CONPORTOS) compete a incumbência pela implantação do Código nas instalações portuárias.

A CONPORTOS é composta pelo Ministério da Justiça, Ministério da Defesa – Comando da Marinha do Brasil (MD/CMB), Ministério da Fazenda (MF), Ministério das Relações Exteriores (MRE), pelo Ministério dos Transportes, Portos e Aviação Civil (MTPA) e, como participante, a Agência Nacional de Transportes Aquaviários (Antaq). Há, ainda, na estrutura da CONPORTOS, as Comissões Estaduais de Segurança Pública nos Portos, Terminais e Vias Navegáveis (CESPORTOS).

Além de regulamentar a implementação do *ISPS Code*, a CONPORTOS tem por objetivo elaborar e implementar o sistema de prevenção e

[1] http://www.imo.org/en/OurWork/Security/SecDocs/Documents/Maritime%20Security/MSC.Circ.443.pdf

[2] http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx

repressão a atos ilícitos nos Portos, Terminais e Vias Navegáveis, por meio de Resoluções e Deliberações.

O Plano de Segurança Pública Portuária (PSP), aprovado pela Comissão em 2002, é um plano de ações cujo objetivo é aperfeiçoar o sistema de segurança pública nos portos, terminais e vias navegáveis, visando reprimir e prevenir o crime e aumentar a segurança. Ao aprovar o PSP, a CONPORTOS emite uma Declaração de Cumprimento (DC) onde atesta que a instalação portuária cumpre as exigências necessárias de acordo com os normativos nacionais e internacionais.

Entretanto, para que este documento esteja alinhado ao *ISPS Code* e às Resoluções da CONPORTOS, faz-se necessário um estudo precedente de avaliação de riscos, assentada às medidas de proteção em função do risco identificado.

É nesse contexto que se insere este trabalho, ao apresentar uma metodologia voltada para a Análise de Riscos com Ênfase na Segurança Portuária (ARESP), alinhada ao *ISPS Code* e às Resoluções da CONPORTOS e que seja, ao mesmo tempo, técnica e transparente.

2. Análise de Riscos com Ênfase em Segurança Portuária (ARESP)

O complexo quadro da segurança portuária brasileira exige técnicas de planejamento, isto é, um estudo que leva em consideração não somente o contexto interno, mas variáveis externas às instalações portuárias, geralmente não controláveis pelos dirigentes.

Ao contemplar um estudo dos ambientes internos e externos, a metodologia ARESP é traduzida como um instrumento técnico de planejamento, pelo que define ações voltadas para a defesa e a segurança física, sendo base para a consolidação de um Plano de Segurança Portuária.

Portanto, na busca pela proteção adequada, a análise de riscos surge como um elemento indispensável nesse cenário dada a sua real capacidade de subsidiar o PSP para o tratamento equilibrado e eficaz da segurança de categorias vulneráveis, como os recursos humanos, a segurança das áreas e instalações, a segurança da central de monitoramento, a segurança dos equipamentos, a segurança da documentação, a

segurança das comunicações e informática, segurança das operações e segurança da informação.

Nesse contexto, a visão proporcionada pela análise de riscos possibilita a seleção de medidas de segurança adequadas que permitam, ao mesmo tempo, que a instalação portuária não seja imobilizada a tal ponto de tornar-se operacionalmente lenta e ineficaz, e que possuam medidas protetivas pertinentes às ameaças que o permeiam. Ou seja, a ARESP procura identificar o equilíbrio necessário entre a segurança, a funcionalidade e o custo.

Do exposto, depreende-se que além de cumprir os requisitos e as diretrizes emanadas pelo *ISPS Code* e pelas resoluções da CONPORTOS, a elaboração de um EAR garante a eficácia e a adequabilidade às medidas e procedimentos de segurança necessários para a proteção de qualquer complexo portuário analisado. Em sentido contrário, a adoção de medidas de segurança sem a necessária análise de riscos e seus respectivos aspectos envolvidos, poderá causar, além do não cumprimento dos normativos nacionais e internacionais, o comprometimento da segurança ao expor as vulnerabilidades decorrentes da insuficiência ou inadequação da implementação de um Plano de Segurança Portuária.

Em resumo, para que uma instalação portuária seja certificada, deve-se efetuar um Estudo de Avaliação de Riscos. Após a sua aprovação, elabora-se um Plano de Segurança Portuária, submetido à CESPORTOS para aprovação. Uma vez implementadas as ações do Plano, realiza-se uma inspeção ou auditoria local e, caso esteja em conformidade, emite-se uma Declaração de Cumprimento (DC). Em ato contínuo, a instalação é incluída no sitio da IMO como Certificada, o que dá a difusão internacional da sua situação.

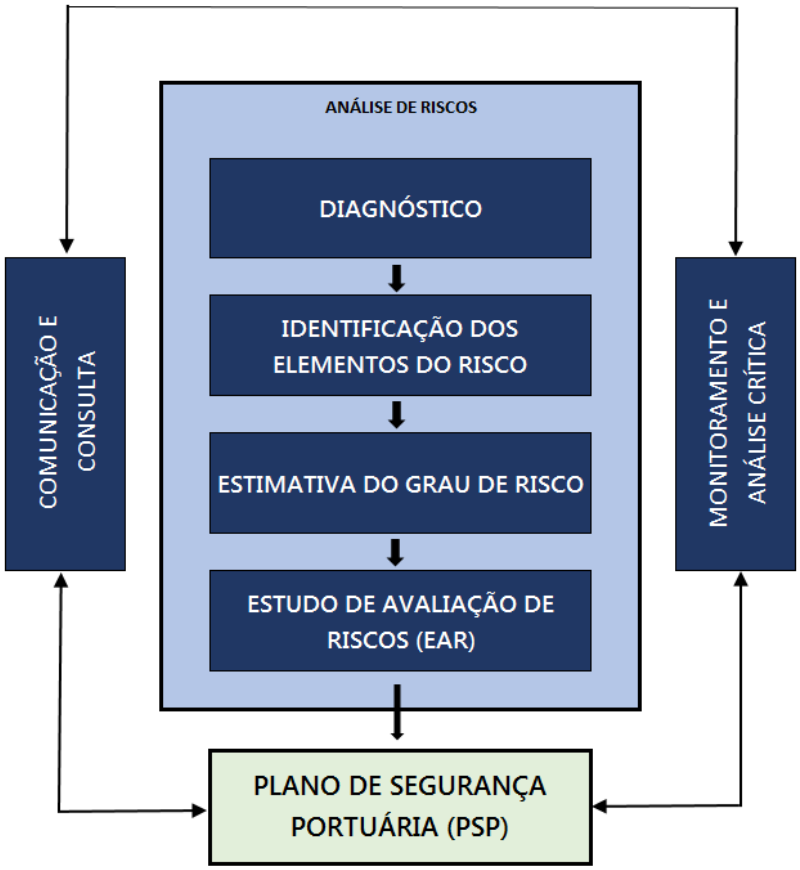
Figura 1 - Processo de emissão da Declaração de Cumprimento



Fonte: Elaborado pelo autor.

Nesse sentido, apresenta-se o framework da metodologia **Análise de Riscos com Ênfase em Segurança Portuária**, com vistas ao assessoramento de possíveis ações preventivas e mitigadoras para a elaboração do Plano de Segurança Portuária:

Figura 2 - Visão Geral do Processo de Gestão de Risco em Segurança Portuária



Fonte: Elaborado e adaptado pelo autor.

2.1 Diagnóstico

O Diagnóstico é a primeira etapa do processo, no qual se realizará um estudo de situação inicial do terminal portuário a ser analisado. Caracteriza-se como um conjunto de técnicas que buscam o aprendizado e a uniformização das informações relacionadas à segurança física das instalações (Andrade, 2017).

Ao considerar que a avaliação de riscos é um processo geral de análise e que ao final apresenta uma relação com os seus principais riscos, apontando a necessidade de um tratamento específico para cada um deles, faz-se necessário que todos

os aspectos de operação de uma instalação portuária sejam contemplados nesta etapa. Assim, determina-se quais setores são mais suscetíveis e/ou prováveis de sofrer um ataque.

Dessa forma, para se estabelecer um Diagnóstico preciso deve-se ter em mente os elementos que deverão ser contemplados. O ISPS aponta, em sua parte B, item 1.17, a necessidade de se incluir as seguintes análises:

1) Determinação da pressuposta ameaça às instalações e infraestrutura do porto;
2) Identificação das prováveis vulnerabilidades;
3) Cálculo das consequências de um incidente.

Além destes três quesitos, o ISPS define que a avaliação da proteção das instalações portuárias deverá incluir, pelo menos, a identificação de avaliação de bens móveis e infraestrutura relevantes, os quais são importantes proteger (item 15.5).

Dessa forma, o risco de proteção é uma função da ameaça de um ataque associado à vulnerabilidade do ativo e as consequências possíveis dessa ação. Extrai-se desses quesitos os elementos que serão analisados detidamente na metodologia ARESP, quais sejam: Ativo, Ameaça, Vulnerabilidades e Consequências; e que deverão ser levados em conta na etapa do Diagnóstico.

Portanto, faz-se necessário realizar um extenso e detalhado mapeamento dos ambientes externo e interno do terminal, cuja finalidade é identificar os elementos que, correlacionados, dão suporte à valoração do risco.

Além das diretrizes elencadas pelo *ISPS Code*, é preciso considerar o rol de procedimentos a serem observados nos estudos de avaliação de risco das instalações portuárias definidos em Resoluções da CONPORTOS. Trata-se de procedimentos imperativos para a aprovação dos estudos de avaliação de risco.

Além de cumprir os requisitos e diretrizes do ISPS e os normativos da CONPORTOS, é preciso compreender e identificar o ambiente no qual o terminal está instalado, sobretudo com relação a: dados de órgãos públicos sobre ocorrências criminais do entorno; informações em fontes abertas; Registros de Ocorrências de Ilícitos Penais (ROIP´s) relacionados aos incidentes de proteção que interferiram nas operações

portuárias ou expuseram em risco a estrutura da instalação e/ou do navio e a integridade das pessoas, ainda que não constituam em ilícitos penais; ocorrências com clandestinos, manifestações e, sobretudo; estudo de vulnerabilidades por meio de uma lista de verificação.

Em resumo, o Diagnótico tem como objetivo fornecer suporte para a próxima etapa - Identificação de Riscos, e deve ser capaz de fornecer subsídios a fim de serem apontadas as ameaças, que podem ser ações naturais e humanas, intencionais ou acidentais e as vulnerabilidades que coloquem em risco os ativos a serem protegidos pela instituição. (ANDRADE, 2017)

O Diagnóstico deve, ainda, buscar compreender como o terminal trata e lida com o assunto segurança física: qual é a política, a cultura organizacional, quais são os princípios e as diretrizes institucionais e qual é o nível de maturidade da instituição para operar com riscos relacionados ao terminal.

Técnicas simples como o uso de *check lists* ou memento de verificação, Entrevista Estruturada e o Brainstorming podem auxiliar o trabalho de elaboração do Diagnóstico.

Convém, ao final do Diagnóstico, proceder à técnica da matriz SWOT[3], na medida em que fornece a possibilidade de visualizar, graficamente, as forças, as fraquezas, as oportunidades e as ameaças relacionadas ao terminal, auxiliando o processo da etapa seguinte: a Identificação dos Riscos.

2.2 Identificação dos Riscos

Para a análise do risco na metodologia ARESP faz-se necessário correlacionar quatro elementos: Ativo, Ameaça/Perigos, Vulnerabilidades e Consequências. Estes são os elementos básicos definidos pelo *ISPS Code*, e podem ser compreendidos da seguinte forma: a Ameaça se vale das Vulnerabilidades para causar Consequências negativas aos Ativos de uma determinada instalação portuária. Portanto, a etapa de Identificação dos Riscos tem como objetivo identificar, avaliar e valorar estes elementos que, correlacionados, definem o grau de risco portuário.

[3] SWOT é a sigla dos termos ingleses Strengths (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças) que consiste em uma metodologia bastante popular no âmbito empresarial.

A CONPORTOS irá elencar os Ativos que deverão, necessariamente, compor o estudo, não sendo, por certo, exaustivo. Além dos Ativos, a Comissão também definirá os itens básicos que aplicar-se-ão em todas as Listas de Verificação. Entretanto, destaca-se que o método de identificação de risco apropriado dependerá da área de aplicação, ou seja, a natureza das atividades e das operações, os requisitos regulatórios, os requisitos do cliente, resultados desejados e o nível requerido de detalhes.

Importa salientar que a valoração dos elementos estruturantes do risco é a etapa mais crítica no processo de avaliação, isto é, quanto melhor a sua compreensão, melhores serão os resultados do processo de avaliação de riscos e mais significativas e eficazes serão as sugestões de tratamento. Ainda, o processo de valoração apresentado pela metodologia ARESP é transparente, e, por conseguinte, torna-se auditável.

Nessa esteira, o ISPS Code, na sua parte A, item 15.3, estabele que:

> As pessoas responsáveis pela execução da avaliação deverão ter os conhecimentos adequados para avaliar a proteção da instalação portuária de acordo com o previsto nesta seção, levando em conta as diretrizes constantes da Parte B deste Código.

2.3 Análise dos Ativos

Ativo deve ser entendido como todo bem que tenha valor para o terminal portuário e pode ser um bem tangível ou intangível. Conforme mencionado, a CONPORTOS irá elencar os Ativos que deverão, necessariamente, compor qualquer Estudo de Avaliação de Riscos.

Entretanto, para que a metodologia ARESP esteja em consonância com o *ISPS Code*, é primordial que os requisitos e as diretrizes do Código sejam obedecidos ao se elaborar a avaliação.

Nesse sentido, a avaliação da proteção das instalações portuárias deverá incluir, pelo menos, a identificação e a valoração de bens móveis e infraestrutura relevantes. Trata-se, portanto, de um processo através do qual se estabelece a importância relativa das estruturas e instalações para o funcionamento da instalação portuária. Este processo de identificação e avaliação fornece uma base para a convergência de estratégias voltadas para a redução do risco, ou para a mitigação do impacto, daqueles bens móveis e estruturas os quais são mais relevantes proteger contra uma ação indesejada.

Ou seja, entender e avaliar o que se quer salvaguardar é fundamental para determinar as consequências de um determinado evento negativo relacionado à segurança, permitindo, por meio da análise de riscos, subsidiar e orientar o responsável quanto a implementação e a priorização das ações corretivas necessárias para se diminuir a possibilidade de ocorrência de eventos futuros indesejados.

A fim de se determinar a importância relativa aos ativos portuários, a ARESP considera as seguintes características: **Substitutibilidade**, **Custo de Reposição** e **Essencialidade (Andrade, 2018).**

A Substitubilidade se refere a qualidade ou condição do que se pretende permutar, ou seja, trata-se da mensuração da condição de facilidade/dificuldade em se substituir um determinado ativo, e é definida em três níveis: Fácil, Média ou Difícil. Trata-se, portanto, de uma avaliação qualitativa com pesos definidos em acordo semântico.

É possível estabelecer faixas por grau definidas quantitativamente, como também proceder à qualificação subjetiva, por meio de votação. Quando ocorrer o segundo caso, quanto mais participantes votarem nesse processo, melhor será a avaliação. Deve-se, por certo, somar a avaliação de todos e dividir pelo número de votantes.

Tabela 1 – Tabela de valoração do ativo: Substitutibilidade

	Substitutibilidade	NOTA
Difícil	3	
Média	2	
Fácil	1	

Fonte: Elaborado pelo autor

O Custo de Reposição pode ser definido quantitativamente ao se estabelecer faixas de valores, tornando-o uma análise quantitativa ou semi-quantitativa. Entretanto, a valoração aqui apresentada dar-se-á de forma qualitativa. A valia do ativo é definido, portanto, de acordo com os seguintes níveis: Baixo, Médio ou Alto.

Tabela 2 – Tabela de valoração do ativo: Custo de Reposição

	Custo de Reposição	NOTA
Alto	3	
Médio	2	
Baixo	1	

Fonte: Elaborado pelos autore

A Essencialidade é a característica do ativo que o torna essecial, isto é, representa o quanto determinado ativo é considerado imprescindível para o cumprimento das funções ou das operações portuárias, devendo ser graduada em três níveis: Alta, Média e Baixa.

Tabela 3 – Tabela de valoração do ativo: Essencialidade

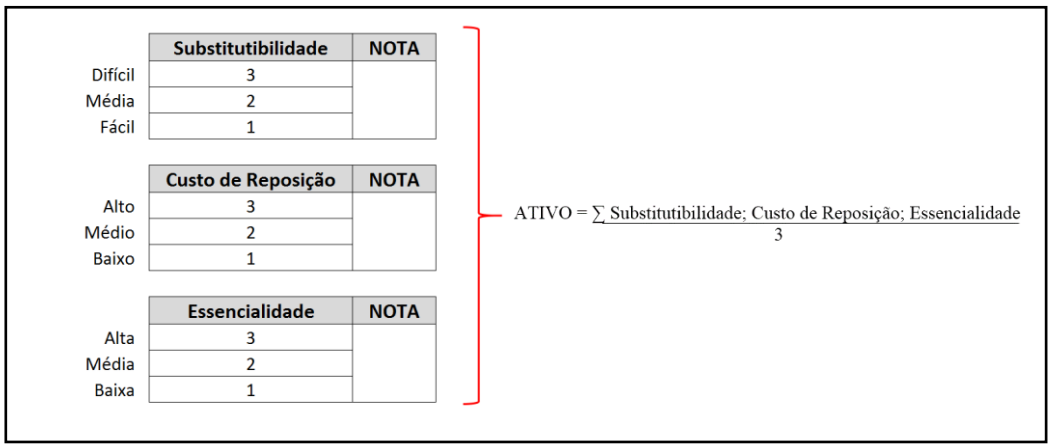
	Essencialidade	NOTA
Alta	3	
Média	2	
Baixa	1	

Fonte: Elaborado pelo autor

Frise-se, mais uma vez, que os responsáveis pela execução da avaliação deverão ter os conhecimentos adequados para valorar os ativos da instalação portuária, ou seja, a análise depende da qualidade das informações para a sua devida classificação.

Finalmente, a nota do Ativo será dada após a determinação dos valores de cada critério considerado, pelo que se faz necessário somar as notas obtidas e dividi-la por 3, devendo ser realizado por Ativo, conforme figura abaixo:

Figura 3 – Valoração do Ativo



Fonte: Elaborado pelo autor

2.4 Análise das Ameaças/perigos

Antes de se apresentar os critérios de valoração das Ameaças e dos Perigos, é preciso discorrer sobre as características destes termos, na medida em que podem gerar certo conflito. A confusão é reflexo da tradução para o português das palavras *safety* e *security* cujo significado, em análise menos detida, significa segurança.

Boholm (2012) comparou o uso e o significado de *safety* e *security* e descobriu que os termos geralmente têm um significado semelhante e, portanto, são frequentemente tratados como sinônimos. No entanto, embora semelhantes, essas palavras também têm significados e aplicações diferentes; e a maioria de seus significados específicos não são compartilhados. Dessa forma, embora o ISPS traga, em suas iniciais, somente o termo *security*, o conteúdo do Código faz menção à questões relacionadas a *safety*.

A diferença básica é facilmente percebida quando associa-se a palavra *security* com ameaça. Isto é, está relacionada a ações naturais como raios, tempestades, tornados, enchentes; ou atos deliberados, intencionais e maliciosos de pessoas, como o crime organizado, funcionários insatisfeitos ou mal-intencionados, terroristas, criminoso comuns, e que colocam em risco os ativos a serem protegidos. Referem-se normalmente à situações externas aos terminais, mas podem fazer parte do contexto interno, como no exemplo de um servidor mal-intencionado.

Safety, por seu turno, esta associado à palavra perigo e aborda a segurança relacionada a riscos acidentais, ou seja, aqueles sem intenção maliciosa, mas com possíveis impactos no ambiente do sistema (Jore, 2017). A falta de manutenção no sistema elétrico, o descuido, ou a má aplicação de equipamentos de trabalho são exemplos de segurança relacionada ao *safety*, ou, para esta metodologia, Perigo.

Geralmente, as Ameaças não são variáveis controláveis. No entanto, em certos casos, as ameaças podem ser neutralizadas, ou, ainda, controladas por meio de ações específicas, executadas, por exemplo, no âmbito dos órgãos de segurança pública. Já os Perigos, por estarem contidos no ambiente interno, geralmente são passíveis de controles e monitoramento.

Há diversas formas de se classificar as Ameaças, seja na forma quantitativa ou qualitativa. Em segurança portuária, contudo, aconselha-se que a análise da Ameaça seja feita utilizando-se o critério qualitativo pelos seguintes motivos: primeiro porque o fato de uma Ameaça nunca ter praticado uma ação indesejada não significa que não o fará; e segundo porque são raros os casos em que as instalações detém dados consolidados sobre incidentes de segurança ocorridos no passado.

Dessa forma, e considerando a complexidade do ambiente portuário, a valoração do nível da Ameaça da metodologia ARESP se dará com base nos seguintes critérios: Motivação, Capacidade e Acessibilidade.

A Motivação se refere a um conjunto de razões que direcionam e influenciam a vontade e a conduta de uma ameaça voltada para a prática de uma ação adversa. A motivação deve ser considerada em função do Ativo, ou seja, qual é o impulso que uma determinada ameaça tem e que faça com ela atinja o seu objetivo – o quanto o Ativo é atrativo para a ameaça. Sua classificação é: Baixa, Média, Alta ou "Não há" (eventos da natureza ou Perigos, por exemplo).

Tabela 4 – Tabela de valoração da Ameaça: Motivação

	Motivação	NOTA
Alta	3	
Média	2	
Baixa	1	
Não há	0	

Fonte: Elaborado pelo autor

Além da necessidade de se considerar o Ativo para a valoração da Ameaça, o analista responsável pela votação deverá, simultaneamente, considerar as possíveis Consequências, ou seja, as ações adversas que podem ser por ela perpretadas. Exemplo:

Tabela 5 – Tabela consolidada de valoração da Ameaça

AMEAÇA: Terrorista - (lobo solitário)				
ATIVO	AÇÕES ADVERSAS	MOTIVAÇÃO	CAPACIDADE	ACESSIBILIDADE
SERVIDORES	Execução de funcionário			
	Ameaça a funcionário			
	Recrutamento			
STS - Porteiner	Roubo/Furto			
	Sabotagem			

Fonte: Elaborado pelo autor

A fim de se valorar a Motivação, o analista deverá proceder da seguinte forma: qual é a motivação que um terrorista (lobo solitário – no exemplo acima) tem para executar um funcionário do porto. Ou, no segundo caso, qual é a motivação que um

terrorista tem em sabotar o porteiner. Decerto que a votação deverá ser valorada de acordo com cada Ativo e considerando cada uma das ações adversas definidas no estudo.

A Capacidade se refere à qualidade que a Ameaça tem para atingir determinado ativo, isto é, o nível de habilidade em termos de condições técnicas, quantidade de elementos, recursos e logísticas que se dispõe, efetivamente, para executar uma ação adversa. O acordo semântico é definido da seguinte maneira: Baixa (1), Média (2) ou Alta (3).

Tabela 6 – Tabela de valoração da Ameaça: Capacidade

	Capacidade	NOTA
Alta	3	
Média	2	
Baixa	1	

Fonte: Elaborado pelo autor

A Acessibilidade é o último critério adotado para a valoração da Ameaça e diz respeito ao nível de acesso que ela dispõe em relação a um determinado Ativo, podendo ser mensurado, direta ou indiretamente, de acordo com os seguintes níveis: Baixa, Média e Alta.

Tabela 6 – Tabela de valoração da Ameaça: Capacidade

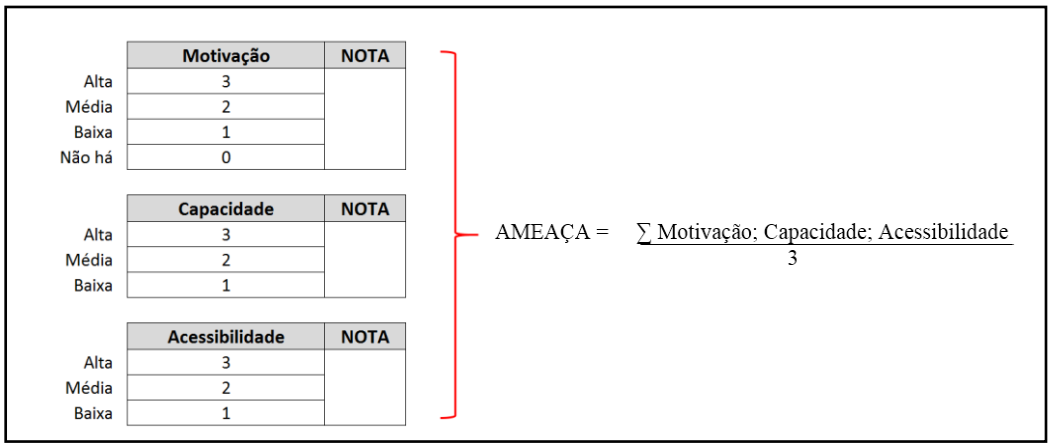
	Acessibilidade	NOTA
Alta	3	
Média	2	
Baixa	1	

Fonte: Elaborado pelo autor

Quando um Ativo for um bem intangível, como por exemplo, a imagem ou a credibilidade institucional, a valoração do nível de acesso deverá ser aferida de forma indireta, devendo-se considerar a acessibilidade da Ameaça em relação ao bem que seria atingido diretamente pela ação adversa. (Andrade, 2018)

A consolidação da votação dos critérios relacionados à Ameaça segue o mesmo rito efetuado no caso dos Ativos: após a determinação dos valores de cada critério para uma determinada Ameaça, deve-se somar as notas e dividí-la por 3.

Figura 3 – Valoração da Ameaça



Fonte: Elaborado pelo autor

Ressalte-se que o procedimento para a mensuração da Ameaça deve se dar de forma individualizada em relação a cada um dos ativos, levando-se em consideração cada uma das respectivas ações adversas. (vide Tabela 5).

2.5 Análise de Vulnerabilidades

Esta etapa é bastante importante porque é a forma mais factível de se reduzir o nível de risco de uma instalação portuária. De forma bastante cartesiana, existem duas maneiras em se reduzir o grau do risco: a primeira é controlar e/ou neutralizar a ameaça; a segunda é minimizar as vulnerabilidades.

Conforme visto, as Ameaças encontram-se, geralmente, no ambiente externo à instalação portuária e extrapolam (e limitam), as possibilidades de ações preventivas – não é razoável atribuir aos terminais a função de atuar sobre uma organização criminosa, investigando-a ou eliminando-a, por exemplo. Por outro lado, as vulnerabilidades representam o principal elemento sobre o qual o gestor pode atuar para reduzir ou mitigar o risco. Com efeito, quando se trata de gestão de risco em segurança portuária, é normalmente atuando sobre as vulnerabilidades que se torna possível modificar a equação do risco.

Neste contexto, a análise da Vulnerabilidade é fundamental e deve ser bem detalhada. Para a sua efetiva identificação, a metodologia ARESP recomenda utilizar uma Lista de Verificação (*Check List*). Convém segmentar o estudo em categorias vulneráveis a fim de se verificar quais apresentam as fragilidades mais significativas. A

CONPORTOS estabelecerá uma Lista de Verificação mínima e categorizada, abordando os itens que, necessariamente, deverão compor a análise.

Não obstante à Lista apresentada pela Comissão, o procedimento de elaboração do *check list* deve ser adaptado para cada terminal de forma a tratar minuciosamente todo o ambiente. Ou seja, a confecção da Lista de Verificação sofrerá influência de acordo com as caracteríticas da instalação portuária ao considerar, por exemplo, os tipos de carga, se tem movimentação de passageiros, áreas de estocagem, os serviços prestados e atividades desenvolvidas, o tráfego e o tipo de embarcações que frequentam a instalação, vigilância terceirizada etc.

Como resultado, torna-se possível identificar, de forma mais clara, a vulnerabilidade de cada uma das categorias - e quais são as respecivas falhas, fragilidades e deficiências do sistema de segurança portuária.

Ao padronizar a Lista de Verificação, o responsável deverá valorar cada item de acordo com a tabela abaixo:

Tabela 7 – Tabela de referência para valoração da Vulnerabilidade

VULNERABILIDADE	DESCRIÇÃO	NOTA
Muito Baixa	O controle existe e é perfeitamente adequado e eficiente	0,5
Baixa	O controle existe, mas a sua adequação e eficiência demandam pequenos ajustes na forma de execução	1
Média	O controle existe, mas a sua adequação e eficiência demandam significativos ajustes na forma de execução	2
Alta	Não existe o controle ou o controle utilizado é completamente inadequado e ineficiente (demanda substituição completa do controle)	3

Fonte: Elaborado pelo autor

Após a valoração dos ítens da Lista de Verificação, deve-se proceder à nota de Vulnerabilidade encontrada por categoria. Para tanto, divide-se o somatório das notas obtidas em todos os itens de cada categoria pelo número de itens checados na categoria. Este procedimento permite-nos obter o Fator Vulnerabilidade de cada categoria (FVc).

$$\text{Fator Vulnerabilidade categoria (FVc)} = \sum \frac{\text{notas itens categoria}}{\text{nº itens checados.}}$$

Como um Plano de Segurança Portuária refere-se ao sistema de proteção de toda a instalação, o passo seguinte é verificar o quanto esse sistema é vulnerável, isto é, o Fator Vulnerabilidade do Sistema (FVS). Logo, o FVS é definido pela soma das notas dos FVc dividido pelo número de categorias vulneráveis.

$$\text{Fator Vulnerabilidade Sistema (FVS)} = \frac{\sum \text{notas FVc}}{\text{nº de categorias vulneráveis}}$$

Ao segregar o estudo das Vulnerabilidades por categorias torna-se possível identificar quais são os itens que contribuíram para uma possível nota alta, ou seja, por meio da análise das vulnerabilidades decorre a base para as recomendações de ações preventivas ou mitigadoras. Conforme visto, é na diminuição da vulnerabilidade que se deve focar o PSP, pois é atuando sobre esta componente que o supervisor de segurança encontra alternativas eficientes e capazes de se reduzir o nível de risco.

2.6 Análise das Consequências

O *ISPS Code*, no ítem 15.10, indica que uma avaliação deverá determinar "As possíveis consequências de um ataque nas instalações portuárias em termos de perda de vidas, danos a propriedades, danos econômicos, incluindo interrupção dos sistemas de transporte".

Nesse contexto, a consequência baseia-se na valoração do Ativo e da sua importância para as atividades de negócios, pelo que, para se alcançar a conformidade com o ISPS Code, é preciso considerar (item 15.5, parte B): "a perda potencial de vidas, a importância econômica do porto, seu valor simbólico e a presença de instalações governamentais".

A metodologia ARESP considera a avaliação dos efeitos que um determinado ativo pode vir a sofrer no caso do risco se concretizar, ou seja, a componente consequência influirá no risco final.

Portanto, atesta-se a conformidade com o ISPS na medida em que a ARESP analisa o quanto um determinado ativo pode ser impactado por diferentes eventos adversos. Dessa forma, a análise das consequências se dará em função da valoração dos efeitos negativos causados a um Ativo pela ocorrência das ações adversas possíveis de

serem praticadas por uma determinada Ameaça, valendo-se das Vulnerabilidades do sistema de segurança portuárias. Percebe-se, mais uma vez, o correlação dos elementos do risco na metodologia apresentada.

As consequências são, na verdade, a classificação em função das ações adversas, identificadas previamente na análise das Ameaças. A sua categorização dar-se-á com base nos seguintes critérios:

Tabela 8 – Critérios para valoração da Consequência

CRITÉRIOS PARA VALORAÇÃO DAS CONSEQUÊNCIAS		
GRAU	**NOTA**	**DESCRIÇÃO**
ALTA	**3**	1. Destruição ou dano irreparável de equipamentos ou instalações
		2. Compromete significativamente os recursos financeiros da instalação
		3. Morte, invalidez permanente, risco de vida ou necessidade de tratamento hospitalar emergencial
		4. Perda ou suspensão da capacidade de operação de atividades essenciais
		5. Compromete a imagem da instituição, com impactos negativos no ambiente interno e/ou externo
		6. Abala consideravelmente o moral de um número significativo de funcionários, ocasionando redução do ritmo e a intensidade das atividades funcionais.
MÉDIA	**2**	1. Dano significativo recuperável de equipamentos ou instalações
		2. Compromete os recursos financeiros da instalação
		3. Não há risco de vida imediato; vítimas com necessidade de tratamento médico hospitalar não emergencial
		4. Perda ou suspensão da capacidade de operação de atividades secundárias (de apoio)
		5. Ocasiona desgaste temporário para a imagem da instituição, mas não compromete a confiança na instituição
		6. Abala o moral de funcionários, sem reduzir o ritmo e a intensidade das atividades funcionais.
BAIXA	**1**	1. Danos sanados pela manutenção orgnâcia de equipamentos ou instalações
		2. Não compromete de forma significativa os recursos financeiros da instalação
		3. Não há risco de vida; vítimas com ferimentos leves tratáveis no próprio local
		4. Interferência ou tumulto em processos internos; sem paralisação ou suspensão de qualquer atividade
		5. Não repercute sobre a imagem da instituição
		6. Não afeta o moral dos funcionários

Fonte: Elaborado pelo autor

Todo PSP tem, como objetivo, a análise voltada para a segurança dos Ativos da instalação portuária. Dessa forma, para preparar a tabela consolidada de riscos, convém destacar o Ativo no topo da tabela e elencar todas as Ameaças e suas subjacentes ações adversas. A seguir, exemplo aplicado para a classificação das consequências:

Tabela 9 – Exemplo de valoração da Consequência

SERVIDORES			
AMEAÇA	**AÇÃO ADVERSA**	**CONSEQUÊNCIA**	**NOTA**
TERRORISTA LOBO SOLITÁRIO	Execução de servidores	ALTA	3
	Ameaça a servidores	MÉDIA	2
	Recrutamento	ALTA	3

Fonte: Elaborado pelo autor

2.7 Estimativa do Grau de Risco

É consenso no meio acadêmico que o risco é conceituado pela combinação da probabilidade de um evento ocorrer e, em ocorrendo, os impactos que ele causaria. Dessa forma, o produto da probabilidade e do impacto é normalmente a maneira mais usual de se obter a caracterização do risco.

Nesse contexto, para a análise da probabilidade de um evento ocorrer, a metodologia ARESP considera o somatório do Fator Vulnerabilidade do Sistema (FVS) com o valor da Ameaça, divido por 2, conforme a seguinte equação:

$$\textbf{(I)} \quad \textbf{PROBABILIDADE} = \frac{\textbf{FVS + Ameaça}}{\textbf{2}}$$

O processo para o cálculo do impacto, por sua vez, é o somatório das notas obtidas pelo Ativo e pela Consequência, divido por 2, conforme exposto abaixo:

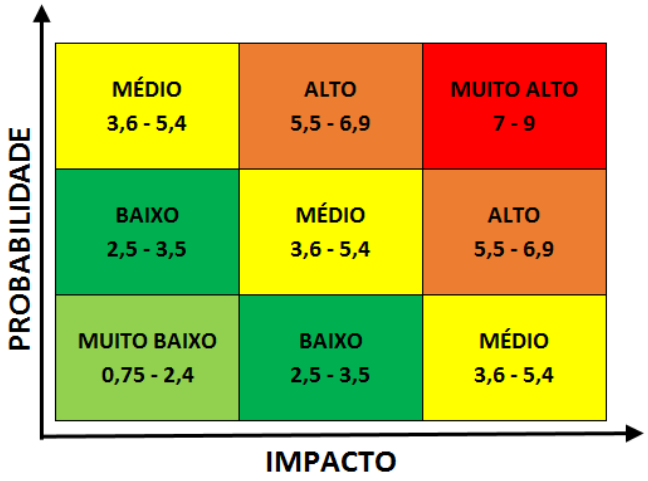
$$\textbf{(II)} \quad \textbf{IMPACTO} = \frac{\textbf{Ativo + Consequência}}{\textbf{2}}$$

Uma vez identificados e mensurados os componentes do risco por meio das notas dos Ativos, das Ameaças, do Fator Vulnerabilidade do Sistema e das Consequências, torna-se possível obter a valoração do risco. Considerando, portanto, que o **Risco = Probabilidade x Impacto**, tem-se:

$$\textbf{(III)} \quad \textbf{RISCO} = \frac{\textbf{FVS} + \textbf{Ameaça}}{\textbf{2}} \times \frac{\textbf{Ativo} + \textbf{Consequência}}{\textbf{2}}$$

Finalmente, o grau do Risco é definido de acordo com os critérios utilizados na metodologia e apresentados em uma Matriz de Risco. A Matriz de Risco da metodologia ARESP é definida em 5 possíveis estágios:

Figura 4 – Matriz de Riscos



Fonte: Elaborado pelo autor

Logo, para a obtenção do grau de risco deve-se associar o valor da equação III com a matriz de risco acima apresentada. Por conseguinte, medidas preventivas deverão ser adotadas em função do resultado encontrado.

O risco pode ser apresentado de forma agrupada, ou seja, com base no valor médio das Ameaças, do Fator de Vulnerabilidade do Sistema, do valor médio dos Ativos e do valor médio das Consequências. Com base neste procedimento, apresenta-se o Risco Agrupado (RA) da instalação portuária como um todo, por meio da seguinte equação: RA = (nota médias das Ameaças + FVS) / 2 x (nota média dos Ativos + nota média das Consequências) / 2.

No entanto, ao se agrupar o risco por meio de médias, fatalmente o terminal portuário irá ocultar riscos mais altos, na medida em que esse processo não considera os extremos – e são, sobretudo, os riscos mais altos que se pretende identificar.

Para o Estudo de Avaliação de Riscos convém, além de identificar o Risco Agrupado, que as análises sejam identificadas por Ativos, destacando-se as Ameaças e as Consequências. Este é o procedimento indicado pela CONPORTOS, haja vista que o risco depende diretamente da Ameaça, sendo possível ocultar uma análise quando feita por meio de médias. Abaixo segue quadro exemplificativo da estrutura final da análise, com foco no Ativo:

Tabela 13 – Tabela de Valoração de Riscos Detalhado

ATIVO:										
PROBABILIDADE				IMPACTO				RISCO	
FATOR VULNERABILIDADE	AMEAÇA	NOTA AMEAÇA	NOTA PROBABILIDADE	AÇÃO ADVERSA	CONSEQUÊNCIA	NOTA DO ATIVO	NOTA IMPACTO	GRAU DO RISCO	CLASSIFICAÇÃO
			0				0	0	ALTO
			0				0	0	MÉDIO
			0				0	0	BAIXO
			0				0	0	ALTO
			0				0	0	MÉDIO
			0				0	0	MUITO ALTO
			0				0	0	MÉDIO
			0				0	0	BAIXO

Fonte: Elaborado pelo autor

Ao detalhar a representação dos riscos por Ativo, o responsável pela análise tem maior condição de perceber o ambiente de forma sistêmica, contextualizada e inter-relacionada, pois todos os aspectos essenciais envolvidos no estudo estão particularizados.

Com reflexo, é possível apontar quais os itens de categorias vulneráveis devem ser melhorados e priorizados em um Plano de Segurança Portuária. Para tanto, basta verificar, junto às categorias vulneráveis (na Lista de Verificação), aqueles que obtiveram uma nota de avaliação mais alta. Dessa forma, o responsável pela segurança terá a capacidade de indicar as contramedidas e os procedimentos mais adequados capazes de interferir de forma efetiva na equação do risco através da redução dos índices de vulnerabilidade.

É por meio deste Estudo de Avaliação de Riscos que o responsável pela segurança terá suporte para a implementação de medidas no PSP, pois servirá para definir e ajustar o grau de rigor das medidas e procedimentos de segurança que deverão compô-lo, equilibrando o emprego dos recursos à proteção efetiva dos ativos portuários.

3. CONCLUSÃO

Por força de resoluções e normativos internacionais, a segurança portuária deve envolver diversas práticas e rotinas, que, consolidadas, geram o Plano de Segurança Portuária. Entretanto, para ter validade, este Plano necessita de uma análise prévia: trata-se do Estudo de Avaliação de Riscos.

A Análise de Riscos com Ênfase em Segurança Portuária, aqui apresentada, atende a estes requisitos e diretrizes ao empregar uma metodologia estruturada, capaz de garantir, a partir de uma visão sistêmica, a eficácia e adequabilidade às medidas e procedimentos necessários.

Portanto, a ARESP orienta a elaboração de normas de segurança, de planos de contingência, de planos de emergência, elaboração de protocolos de segurança e de procedimentos essenciais não somente para a obtenção da Declaração de Cumprimento, por meio do PSP, mas para garantir a base para as medidas de proteção das instalações portuárias brasileiras em função do risco identificado..

BIBLIOGRAFIA

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 31000/2009. **Gestão de Riscos – Princípios e diretrizes**, ABNT, 2009.

_____ NBR ISO/IEC 31010/2012. **Gestão de Riscos – Técnicas para o processo de avaliação de riscos**, ABNT, 2012.

ANDRADE, Felipe Scarpelli**. Análise de Riscos e a Atividade de Inteligência.** Revista Brasileira de Ciências policiais. 2017. Disponível em: < https://periodicos.pf.gov.br/index.php/RBCP/article/view/462/311> Acesso em 13 de julho de 2018.

ANDRADE, F.S., ROCKEMBACH, S. J. **Metodologia ARSO: Análise de Riscos em Segurança Orgânica**. Revista Mercopol. Edición Paraguay. Año XI, nº11. ISSN 2236-9236. 2018.

AVEN, Terje. **Foundations of Risk Analysis**. Wiley, 2012.

BADREDDINE, A., Amor, N.B.: **A Bayesian approach to constructo bow tie diagrams for risk evaluation.** Process Safety and Environmental Protection 91(3), 159-171 (2013).

BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade.** Tradução de Sebastião Nascimento. São Paulo: Ed. 34, 2011.

BERG, Heinz-Peter. **Risk Management: Procedures, Methods and Experiences.** RT&A, 2, 2010.

BOHOLM, M. (2012). **The semantic distinction between "risk" and "danger": A linguistic analysis**. Risk Analysis, 32(2), 281–293.

BRODER, James F. and TUCKER, Eugene. **Risk Analysis and the Security Survey.** Elsevier, 2012.

International Ship Suppliers & Services Association. International Ship And Port Facility Security Code. **ISPS Code guidelines for Ship Suppliers.** 2016.

JORE, S.H. **The risk and value nexus in security risk management.** Safety and Reliability – Theory and Applications – epin & Briš (Eds). 2017.

LANDOLL, Douglas J. **The Security Risk Assessment Handbook. Auerbach Publications,** New York, 2006.