Felipe Scarpelli

Metodologia ARESP

METODOLOGIA, APLICAÇÃO E AS PARTICULARIDADES DA ARESP

Análise de Risco com Ênfase em Segurança Portuária

Participação:
Dr. Marcelo João - Presidente da CONPORTOS
Felipe Scarpelli de Andrade - Polícia Federal
CMG Paulo Barros - Oficial de ligação da MB na CONPORTOS

30 de junho| 10h às 12h
Transmissão pelo Microsft Teams

ATP

Análise de Riscos com Enfase em Segurança Portuária

O ISPS Code, item 1.17 parte B:

A avaliação de proteção é fundamentalmente uma análise de riscos de todos os aspectos de operação de uma instalação portuária a fim de determinar quais partes dela são mais suscetíveis, e/ou prováveis de sofrer um ataque. O risco de proteção é uma função da ameaça de um ataque, juntamente com a vulnerabilidade do alvo e as consequências de um ataque.

A avaliação deve incluir os seguintes itens:

- determinação da pressuposta ameaça às instalações e infraestrutura do porto;
- identificação das prováveis vulnerabilidades; e
- cálculo das consequências de um incidente.

Internacionalmente, o risco é conceituado pela combinação da probabilidade de um evento e suas consequências. Probabilidade e consequência são os dois elementos que caracterizam o risco. Entretanto, o ISPS Code acrescentou mais um ingrediente para a avaliação de riscos que é a vulnerabilidade. Para se identificar a **evidência de conformidade**, esses três ingredientes (probabilidade, consequência e vulnerabilidade) devem fazer parte desse processo.

Risco = PROBABILIDADE X IMPACTO

ISPS item 15.5

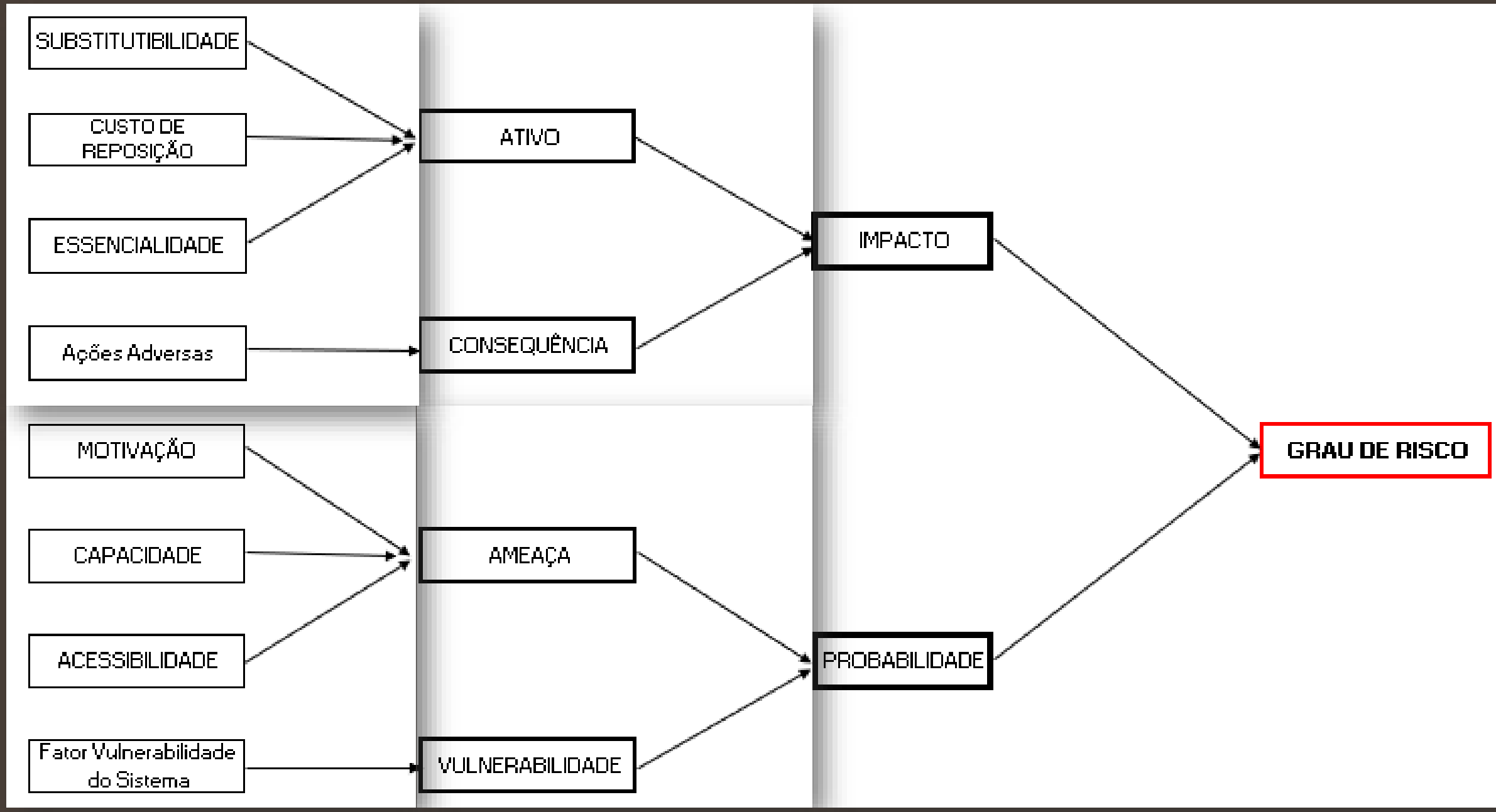
A avaliação da proteção das instalações portuárias deverá incluir, pelo menos, os seguintes elementos:

1. Identificação e avaliação de bens móveis e infraestrutura relevantes, os quais são importantes proteger;

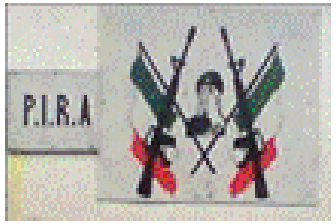
2. Identificação de possíveis ameaças a bens móveis e infraestrutura e a possibilidade de sua ocorrência, a fim de estabelecer e priorizar medidas de proteção;

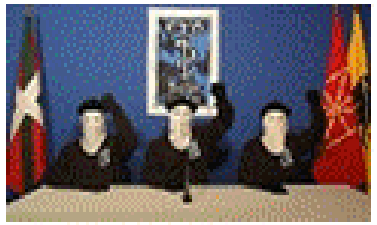
3. Identificação, seleção e priorização de contramedidas e alterações nos procedimentos e seu nível de eficácia quanto à redução de vulnerabilidade; e

4. Identificação de fraquezas, incluindo fatores humanos, na infraestrutura, planos de ação e procedimentos.


SUBSTITUTIBILIDADE
CUSTO DE REPOSIÇÃO
ESSENCIALIDADE
Ações Adversas
ATIVO
CONSEQUÊNCIA
IMPACTO
MOTIVAÇÃO
CAPACIDADE
ACESSIBILIDADE
Fator Vulnerabilidade do Sistema
AMEAÇA
VULNERABILIDADE
PROBABILIDADE
GRAU DE RISCO

Ameaças

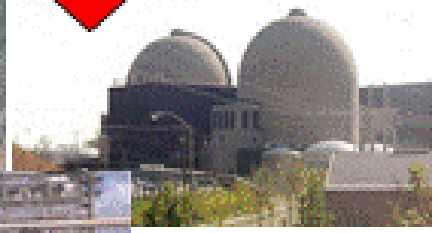


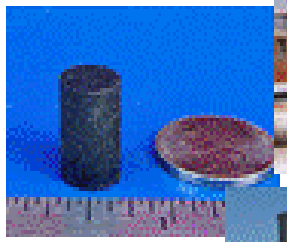


Consequências

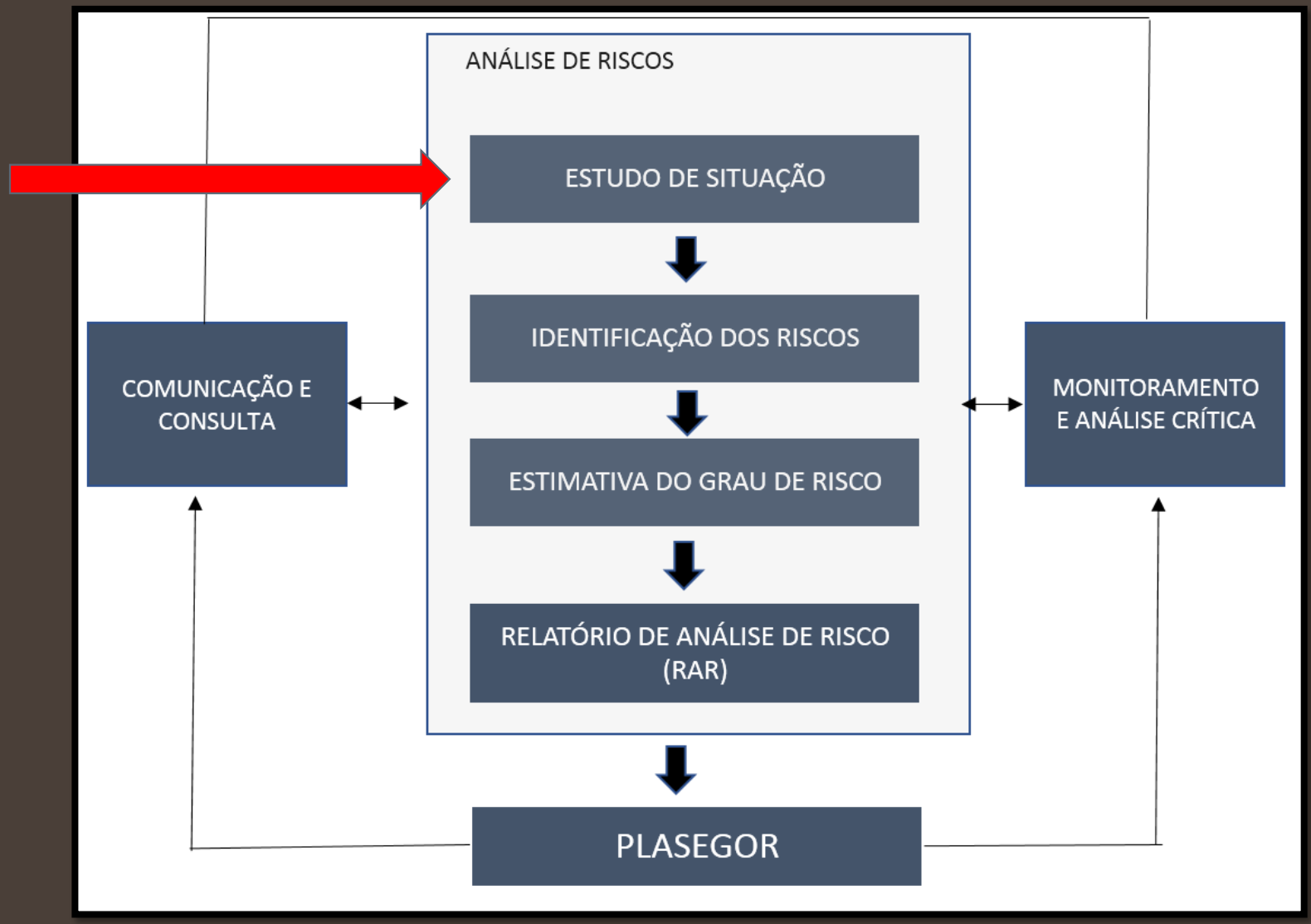
Sistema de Proteção Física

Alvos





ARESP – Framework



Estudo de Situação

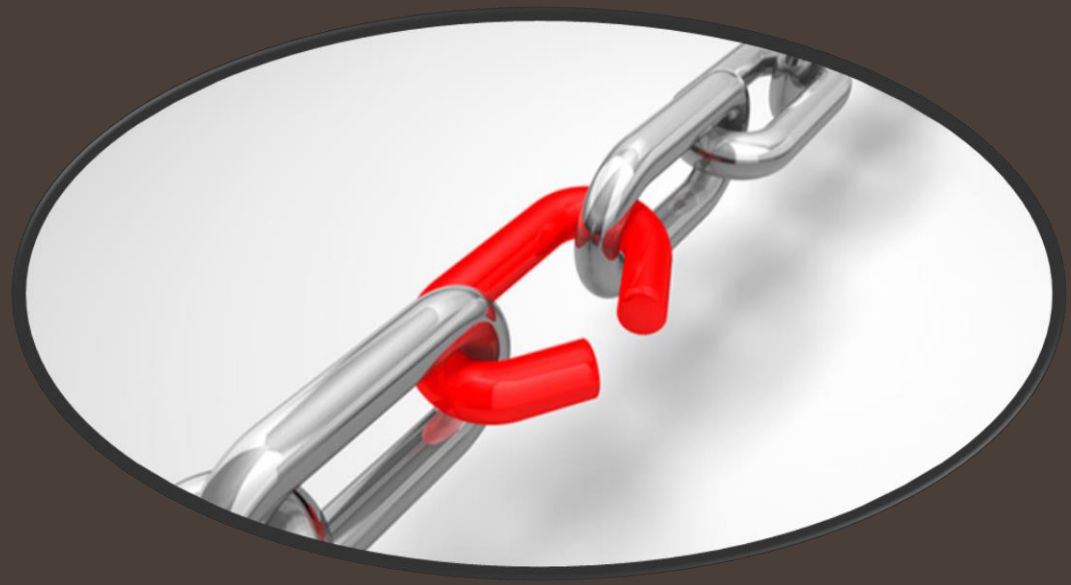
O Estudo de situação é a primeira etapa do processo, no qual se realizará um diagnóstico inicial do sistema a ser analisado. O objetivo aqui é fornecer suporte para a próxima etapa (“Identificação de Riscos”) por meio de técnicas capazes de apontar as ameaças que podem ser ações naturais e humanas, intencionais ou acidentais; e as vulnerabilidades que coloquem em risco os ativos a serem protegidos pela instituição. (ANDRADE, 2017)

AMBIENTE INTERNO

AMBIENTE EXTERNO

Estudo de Situação

Para o Estudo de Situação, o responsável pode-se valer de diversas técnicas, como Entrevista Estruturada ou um Memento de Levantamento de Vulnerabilidades. Deve-se utilizar, como apoio, a Resolução da CONPORTOS Nº 52.



ENTREVISTA ESTRUTURADA

Um conjunto de perguntas é criado para orientar o entrevistador.

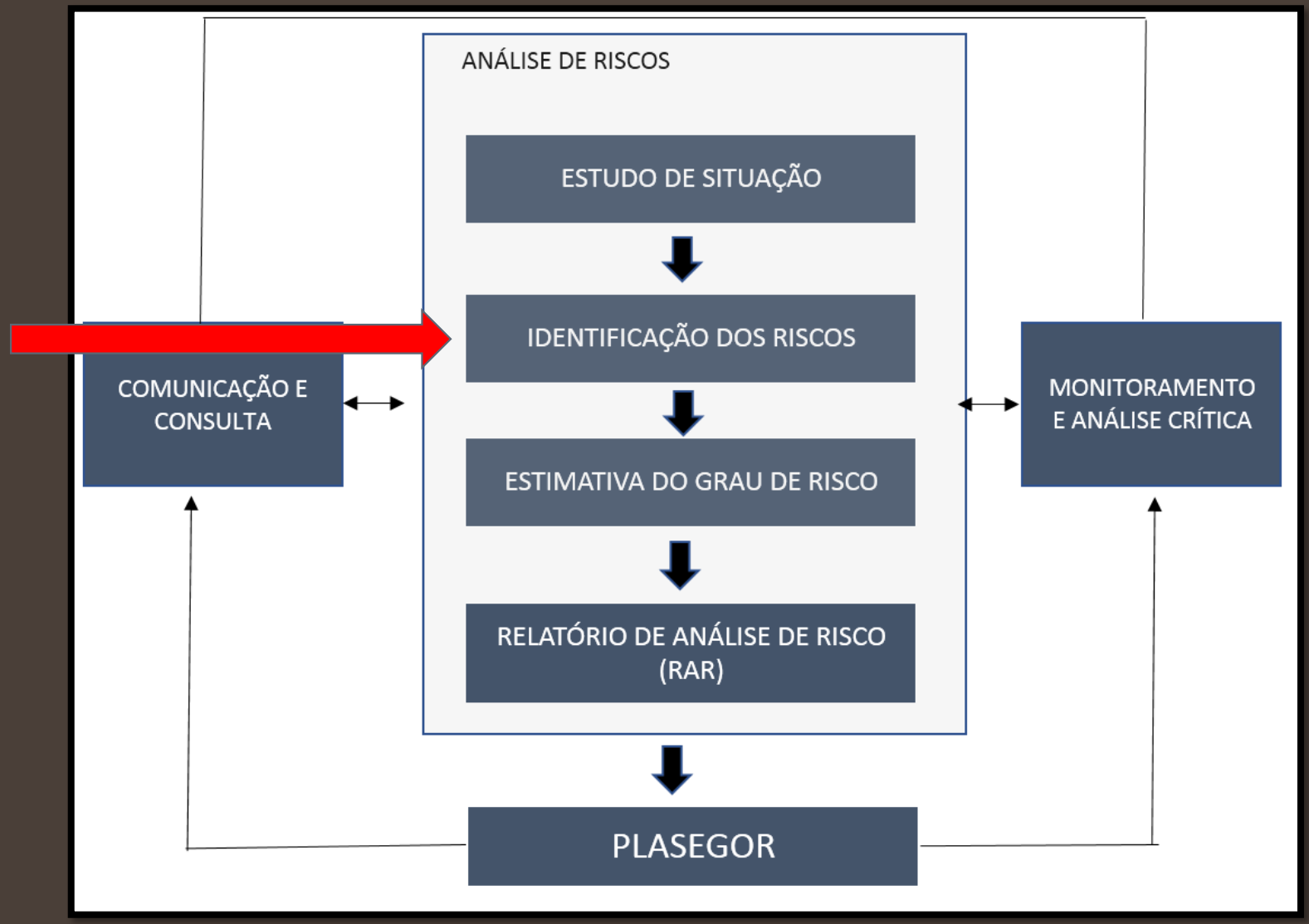
As perguntas podem ser abertas ou fechadas. Entretanto, sempre que possível, recomenda-se fazê-las de modo que as respostas sejam consideradas com um certo grau de flexibilidade, a fim de dar a oportunidade ao entrevistado de explorar as áreas que desejar.

ENTREVISTA ESTRUTURADA

LEVANTAMENTO DE VULNERABILIDADES

1. Segurança das Áreas e Instalações

I. SISTEMA DE BARREIRA FÍSICA	OBSERVAÇÕES
Limite perimetral (externo) definido e cercado por sistema de barreiras	
Barreira perimetral com sinalização externa;	
Sistema de barreiras perimetrais sem solução de continuidade;	
Trechos mais críticos das barreiras perimetrais integrados com alarmes e/ou sensores de detecção (intrusão)	
Trechos mais críticos das barreiras perimetrais submetidos a rondas	
Trechos mais críticos das barreiras perimetrais monitorados por CFTV	
Trechos mais críticos das barreiras perimetrais empregam utilização de corredor técnico	


ANÁLISE DE RISCOS
ESTUDO DE SITUAÇÃO
IDENTIFICAÇÃO DOS RISCOS
ESTIMATIVA DO GRAU DE RISCO
RELATÓRIO DE ANÁLISE DE RISCO (RAR)
COMUNICAÇÃO E CONSULTA
MONITORAMENTO E ANÁLISE CRÍTICA
PLASEGOR

Identificação dos Riscos

Esta fase tem por finalidade identificar e avaliar os elementos dos risco, isto é, analisar os ativos, as ameaças, as vulnerabilidades e as consequencias negativas da ocorrência de um evento indesejado.

Elementos do Risco da metodologia ARESP

A Análise do Risco é a correlação entre esses três elementos

E qual a fórmula a se utilizar?

Correlação dos Elementos do Risco

Risco = PROBABILIDADE X IMPACTO

Sendo que:

$$\textbf{PROBABILIDADE} = \frac{\textbf{Fator Vulnerabilidade} + \textbf{Nível de Ameaça}}{\textbf{2}}$$

$$\textbf{IMPACTO} = \frac{\textbf{Ativo} + \textbf{Consequência}}{\textbf{2}}$$

Correlação dos Elementos do Risco

A valoração dos elementos estruturantes do risco é a etapa mais crítica no processo de avaliação de risco: 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.

Ativos

15.5 A identificação e avaliação da infraestrutura e bens móveis importantes é um processo através do qual se pode estabelecer a importância relativa das estruturas e instalações para o funcionamento da instalação portuária. Este processo de identificação e avaliação é importante porque fornece uma base para a concentração de estratégias de atenuação do impacto naqueles bens móveis e estruturas os quais são mais importantes proteger contra um incidente de proteção.

Ver item 15.7 ISPS Code.

Os **Ativos** são os bens a serem protegidos. Tudo que tenha valor para a organização

- Pessoas
- Edificações
- Equipamentos
- Produção imaterial
- Produção material
- Informações
- Imagem institucional

E como analisar meu Ativo?

Há diversas formas de se classificar um ativo. Aqui, se dará em função de três características: **Substitutibilidade**, **Custo de Reposição** e **Essencialidade**, conforme exemplo:

	Substitutibilidade	Nota
Difícil	3	
Média	2	
Fácil	1	

	Custo de Reposição	Nota
Alto	3	
Médio	2	
Baixo	1	

	Essencialidade	Nota
Alta	3	
Média	2	
Baixa	1	

A Substitubilidade refere-se à mensuração da condição de facilidade/dificuldade em se substituir um determinado ativo: Fácil, Médio ou Difícil. É possível estabelecer faixas por grau definidas quantitativamente, como também proceder à qualificação subjetiva, por meio de votação

O Custo de Reposição trata, subjetivamente, da valia do ativo e é definido de acordo com os seguintes níveis: Baixo, Médio ou Alto.

A Essencialidade representa o quanto determinado ativo é considerado indispensável para o cumprimento das funções e missões institucionais, bem como para a consecução dos objetivos estratégicos corporativos, podendo ser graduada em três níveis: Alta, Média e Baixa

Ativos

A Substitubilidade refere-se à mensuração da condição de facilidade/dificuldade em se substituir um determinado ativo: Fácil, Média ou Difícil. 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.

SUPERVISOR DE SEGURANÇA				
Substitutibilidade	**Nota 1**	**Nota 2**	**Nota 3**	**Valor**
3	2,5	2,7	3	2,73333
2				
1				

Ativos

O **Custo de Reposição** trata, subjetivamente, da valia do ativo e é definido de acordo com os seguintes níveis: Baixo, Médio ou Alto. Assim como na Substitutibilidade, é possível estabelecer um acordo semântico com critérios objetivos, ou seja, criar faixas de valores para cada nível de Custo de Reposíção, tornando-o uma análise quantitativa ou semi-quantitativa.

SUPERVISOR DE SEGURANÇA				
Custo de Reposição	**Nota 1**	**Nota 2**	**Nota 3**	**Valor**
3	2,5	2,5	3	2,66667
2				
1				

Ativos

A **Essencialidade** representa o quanto determinado ativo é considerado indispensável para o cumprimento das funções e missões institucionais, bem como para a consecução dos objetivos estratégicos corporativos, podendo ser graduada em três níveis: Alta, Média e Baixa.

SUPERVISOR DE SEGURANÇA				
Essencialidade	**Nota 1**	**Nota 2**	**Nota 3**	**Valor**
3	2,8	3	2,8	2,86667
2				
1				

Ativos

Após a determinação dos valores de cada critério para um determinado Ativo, deve-se somar as notas obtidas e dividir por 3.

$$\text{ATIVO} = \frac{\sum \text{Substitutibilidade; Custo de Reposição; Essencialidade}}{3}$$

ATIVO	Valor
Supervisor de Segurança	2,75556
Operador de Portêiner	2,41111
Funcionário Administrativo	1,72222

Ameaças/ Perigos

2- Identificação de possíveis ameaças a bens e infraestrutura e a probabilidade de sua ocorrência, a fim de estabelecer e priorizar medidas de proteção

A parte B do código, nos itens 15.9 a 15.12, estabelece as seguintes diretrizes:

15.9 Possíveis atos que possam ameaçar a proteção de bens móveis e infraestrutura e os métodos utilizados para sua execução devem ser identificados para avaliar a vulnerabilidade de um determinado bem móvel ou local em relação a um incidente de proteção e para estabelecer e priorizar os requisitos de proteção a fim de permitir o planejamento e a alocação de recursos. A identificação e avaliação de cada ato potencial e do método utilizado para executá-lo deve ser baseada em vários fatores, incluindo avaliações de ameaças por organizações Governamentais.

Ameaças/ Perigos

Ameaças são ações naturais e humanas, intencionais ou não (acidentes), que colocam em risco os ativos a serem protegidos. Sem ameaça não existe risco!

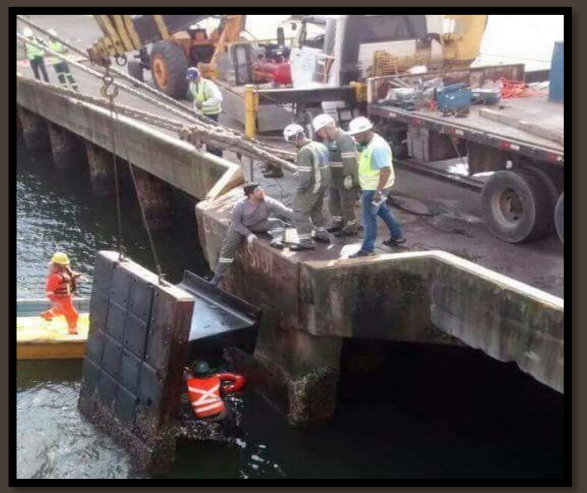
- ERROS HUMANOS
- FUNCIONÁRIOS INSATISFEITOS E COM PROBLEMAS
- CRIMINOSOS COMUNS
- TERRORISTAS
- AÇÕES DO MEIO AMBIENTE
- SABOTADORES ...

A ABNT/ISO/Guia 73 denomina as Ameaças como sendo Fontes de Risco

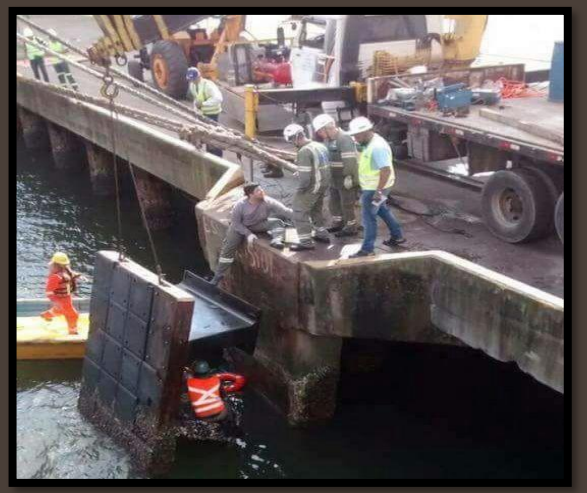
Ameaças/ Perigos

O perigo se refere a situação que tanto pode ser uma ação como uma condição que apresenta o potencial de produzir um dano sobre um determinado ativo. Este dano pode produzir alguma lesão física ou uma doença conforme o caso, ou pode provocar um evento indesejado em uma instalação/ativo específico.

Perigo



Perigo



Ameaças/ Perigos

Exemplificando:

A interrupção do fornecimento de energia (incidente não previsto no ISPS Code) pode ser decorrente de uma descarga elétrica (raio) que, devido a uma falha no equipamento (para-raios); pode ser decorrente de uma ação intencional se provocar a ruptura do cabo condutor, ou por falta de manutenção do equipamento. Esse simples evento pode interromper as atividades de uma instalação portuária e interferir na eficácia do sistema de proteção.

Ameaças/ Perigos

Exemplificando:

O subitem 2 do item 15.7 diz que os bens móveis e a infraestrutura que devem ser considerados podem incluir equipamentos para manuseio de cargas. O portêiner é um equipamento importante e estratégico para um terminal de contêiner (TECON). A interrupção de sua atividade pode decorrer da falta de energia, de modo acidental ou intencional. O evento erro ou falha não é contemplado no ISPS Code, mas é factível, e pode e deve ser considerado. Não considerar os atos (incidentes e ameaças) para esse equipamento, é não atender ao ISPS Code, por não observar o item 15.7 e o 15.9.

15.10 A Avaliação de Proteção das Instalações Portuárias deve incluir uma avaliação realizada em consulta com as organizações nacionais de proteção relevantes para determinar:

1. Quaisquer aspectos particulares das instalações portuárias, incluindo o tráfego de navios que utilizam as instalações, os quais as tornam passíveis de serem alvos de um ataque;

2. 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.

3. A capacidade e intenções daqueles passíveis de planejar tal ataque; e

4. Os possíveis tipos de ataques, realizando uma avaliação completa do nível de risco contra o qual as medidas de proteção têm que ser desenvolvidas.

Ameaças

Concomitantemente à identificação da ameaça, o grupo de analistas deve relacionar quais seriam as ações adversas possíveis de serem praticadas por ela, tendo como foco o ativo que se pretende proteger.

ORCRIM	
ATIVO	**AÇÕES ADVERSAS**
SERVIDORES	Execução de servidores
	Ameaça a servidores
	Recrutamento
INFORMAÇÕES SIGILOSAS	Acesso
	Destruição
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Roubo/Furto
	Sabotagem
INSTALAÇÕES	Acesso não autorizado
	Depredação/Vandalismo
IMAGEM INSTITUCIONAL	Execução de servidores
	Ameaça a servidores
	Acesso Info. Sigilosas
	Infiltração
	Sabotagem Infra Criticas

SERVIDOR INSATISFEITO	
ATIVO	**AÇÕES ADVERSAS**
INFORMAÇÕES SIGILOSAS	Vazar Info. Sigilosas
	Destruir
	Contrafação
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Sabotagem
	Roubo/Furto
INSTALAÇÕES	Facilitar o acesso
IMAGEM INSTITUCIONAL	Vazar Info. Sigilosas
	Facilitar o acesso as A&I
	Roubo/Furto Mat Sens

E como analisar as Ameaças?

Ameaças/ Perigos

As ameaças podem ser classificadas e valoradas de diversas formas. Para a metodologia (EAR), a valoração do nível da ameaça/perigo se dará com base na motivação, na capacidade e na acessibilidade que a ameaça possui para perpetrar ações adversas capazes de atingir um ativo.

	Motivação	Nota
Difícil	3	
Baixo	1	

	Acessibilidade	Nota
Alta	3	
Média	2	
Baixa	1	

IMPORTANTE

O procedimento para a mensuração da ameaça/perigo deve se dar de forma separada em relação a cada um dos ativos, levando-se em consideração cada uma das ações adversas possíveis de serem praticadas pela ameaça considerada, conforme exemplo apresentado a seguir:

E como analisar meu Ativo?

Há diversas formas de se classificar um ativo. Aqui, se dará em função de três características: **Substitutibilidade**, **Custo de Reposição** e **Essencialidade**, conforme exemplo:

	Motivação	Nota
Difícil	3	
Média	2	
Baixa	1	
Não aplicável	NA	

	Capacidade	Nota
Alto	3	
Médio	2	
Baixo	1	

	Acessibilidade	Nota
Alta	3	
Média	2	
Baixa	1	

A **Motivação** refere-se a um conjunto de motivos que direciona e influencia a vontade e a conduta de uma ameaça voltada para a prática de uma ação adversa. Sua classificação é: Baixa, Média, Alta ou "Não Aplicável" motivação (eventos da natureza ou perigos, por exemplo).

A **Capacidade** de uma Ameaça significa o nível de habilidade (condições técnicas, quantidade de elementos, recursos e logísticas) que uma determinada ameaça possui efetivamente para executar uma ação adversa, e é definida da seguinte forma: Baixa, Média ou Alta.

A **Acessibilidade** refere-se ao nível de acesso que a Ameaça possui em relação a um determinado ativo, podendo ser mensurado, direta ou indiretamente, de acordo com os seguintes níveis: Baixa, Média e Alta.

		AMEAÇA: COVID 19									
		MOTIVAÇÃO			CAPACIDADE			ACESSIBILIDADE			Valor Total
ATIVO	AÇÕES ADVERSAS	Nota 1	Nota 2	Nota 3	Nota 1	Nota 2	Nota 3	Nota 1	Nota 2	Nota 3	
Supervisor de Segurança	Óbito	NA	NA	NA	3	3	3	2,5	2	2,5	2,666667
	Afastamento das atividades	NA	NA	NA	3	3	3	2,5	2	2,5	2,666667
											0
ATIVO	AÇÕES ADVERSAS	MOTIVAÇÃO			CAPACIDADE			ACESSIBILIDADE			NOTA
Operador de Portêiner	Óbito	NA	NA	NA	3	3	3	2,5	2	2	2,583333
	Afastamento das atividades	NA	NA	NA	3	3	3	2,5	2	2	2,583333
ATIVO	AÇÕES ADVERSAS	MOTIVAÇÃO			CAPACIDADE			ACESSIBILIDADE			NOTA
Funcionário Administrativo	Óbito	NA	NA	NA	3	3	3	2,5	3	3	2,916667
	Afastamento das atividades	NA	NA	NA	3	3	3	2,5	3	3	2,916667

ORCRIM					
ATIVO	**AÇÕES ADVERSAS**	**MOTIVAÇÃO**	**CAPACIDADE**	**ACESSIBILIDADE**	**NOTA**
SERVIDORES	Execução de servidores	2	2	3	2,3
	Ameaça a servidores	2	2	3	2,3
	Recrutamento	2	2	3	2,3
INFORMAÇÕES SIGILOSAS	Acesso	3	2	1	2
	Destruição	1	2	1	1,3
	Contrafação	1	1	1	1
INFRAESTRUTURAS E MATERIAIS CRÍTICOS	Roubo/Furto	1	1	1	1
	Sabotagem	1	1	1	1
INSTALAÇÕES	Acesso não autorizado	1	1	2	2
	Depredação/Vandalismo	1	3	3	2,3
IMAGEM INSTITUCIONAL	Execução de servidores	2	2	3	2,3
	Ameaça a servidores	2	2	3	2,3
	Acesso Info. Sigilosas	3	2	1	2
	Infiltração	3	3	3	3
	Sabotagem Infra Criticas	2	3	2	2,3

Vulnerabilidades

- As vulnerabilidades estão contidas no contexto interno de uma organização e são o principal elemento no qual o gestor pode atuar para reduzir ou mitigar o risco. Pode ser definida como as fragilidades, as fraquezas ou as insuficiências na segurança física e procedimental de uma determinada instalação.

Vulnerabilidades

Categorias Vulneráveis

- Dispositivos de Detecção e Contenção
- Segurança da Edificação
- Segurança Perimetral
- Segurança de RH
- Eventos Passados
- Funcionários de Segurança
- Política e Procedimentos
- Organização para Emergência

Uma vez definidas, cada categoria deverá ter seus itens analisados e distribuídos, a fim de se obter uma nota, que varia de 0,5 a 3, em função dos seguintes critérios:

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

VULNERABILIDADE Segurança das Instalações

Segurança das Áreas e instalações	Nota
Áreas internas do edifício iluminadas	2
Existem câmeras adequadas no acesso	3
Existem áreas de escape em caso de incêndio	3
Guarita de entrada com checagem individual	2
Controle de entrada e saída de veículos	1
Armazenamento em banco de dados do registro de visitantes e servidores	3
Controle de acesso de todos os funcionários	2
Área interna do edifício é visualizado de fora do complexo	1
Salas de reunião e outros locais sensíveis oferecem segurança para assuntos sensíveis	1
Diretrizes orientando ações quando fatos anormais ocorrem em áreas adjacentes	2
Áreas submetidas, regularmente, a varredura visual e eletrônica	3
TOTAL	23

VULNERABILIDADE	NOTA
Muito Baixa	0,5
Baixa	1
Média	2
Alta	3

Identificação do Fator Vulnerabilidade por categoria

$$\frac{\sum \text{notas itens categoria}}{\text{nº itens checados.}}$$

Segurança das Áreas e instalações	Nota
Áreas internas do edifício iluminadas	2
Existem câmeras adequadas no acesso	3
Existem áreas de escape em caso de incêndio	3
Guarita de entrada com checagem individual	2
Controle de entrada e saída de veículos	1
Armazenamento em banco de dados do registro de visitantes e servidores	3
Controle de acesso de todos os funcionários	2
Área interna do edifício é visualizado de fora do complexo	1
Salas de reunião e outros locais sensíveis oferecem segurança para assuntos sensíveis	1
Diretrizes orientando ações quando fatos anormais ocorrem em áreas adjacentes	2
Áreas submetidas, regularmente, a varredura visual e eletrônica	3
TOTAL	**23**

Soma-se as notas individuais e divide-se pelo número de itens: 23/11 = 2,09

Fator Vulnerabilidade por categoria

$$\frac{\sum \text{notas itens categoria}}{\text{nº itens checados.}}$$

Segurança dos Recursos Humanos	Nota
Pessoas com destaque em mídia	1
Funcionários com problemas financeiros, bebida, drogas, redes sociais	2
Funcionários possuem curso de formação em segurança e emergências	1
Regras escritas sobre normas de segurança	3
Uso de crachá por todos no interior do complexo	3
Processo seletivo dos candidatos a Instituição sofrem investigação social e entrevista	2
A Unidade de Inteligência participa ativamente do processo de seleção dos novos servidores	1
Integrantes da Instituição que têm acesso a assuntos sigilosos assinam Termo de Compromisso de Manutenção do Sigilo	3
Compartimentação referente a assuntos sensíveis entre as diversas funções e cargos desempenhados na Instituição.	2
TOTAL	**18**

18/9 = 2

Fator Vulnerabilidade por categoria

$$\frac{\sum \text{notas itens categoria}}{\text{nº itens checados.}}$$

Segurança das Informações	Nota
Classificação de cargos e funções segundo níveis de sensibilidade	1
Inteligencia participa ativamente dos processo de seleção de pessoal	2
Assinatura do Termo de Compromisso de Sigilo (TCMS)	1
Procedimento normatizado para o credenciamento de segurança	3
Itinerários definidos para o fluxo de funcionarios	3
Itinerários definidos para o fluxo de visitantes	2
Condição de visitante pode ser rapidamente reconhecida por qualquer integrante da instituição	1
Classificação e demarcação física visual dos locais de acesso restrito	3
Procedimentos restritivos quanto a entrada e utilização de cameras, telefones, pendrives, gravadores nas áreas e instalações	2
TOTAL	**18**

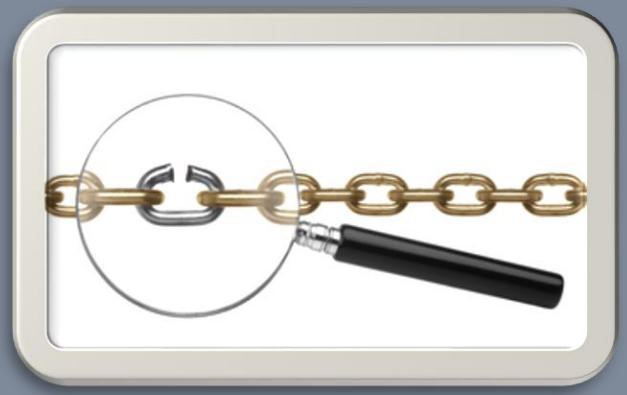
18/9 = 2,0

Fator Vulnerabilidade do Sistema

- Segurança das Instalações – 2,09
- Segurança de Pessoal – 2,0
- Segurança de Áreas externas – 2,0

O fator de vulnerabilidade do exemplo citado é a soma das notas de vulnerabilidade dividido pelo número de categorias: **6,09/3 = 2,03**.

$$\frac{\sum \text{notas FV categoria}}{\text{nº categorias.}}$$



Em segurança orgânica, é normalmente atuando sobre as vulnerabilidades que uma instituição pode modificar a equação do risco.

Portanto, a análise deste componente é fundamental e deve ser bem detalhada.

%Vulnerabilidade relativa da Categoria

O passo seguinte é verificar o quanto vulnerável encontra-se cada categoria em relação as demais.

- ✓ Divide-se a Nota do Fator Vulnerabilidade da Categoria pelo somatório das Notas Categorias x 100

Categoria Vulnerável	Nota	Nota Máxima	% Vulnerabilidade	% Vulnerabilidade Total
Segurança das instalações	2,09	3	34,32%	67,67%
Segurança dos Recursos Humanos	2	3	32,84%	
Segurança das Informações	2	3	32,84%	
Total	**6,09**	**9**	**100,00%**	

$$\%\text{Vulnerabilidade Categoria} = \frac{\text{FV Categoria}}{\sum \text{notas Categorias}} \times 100$$

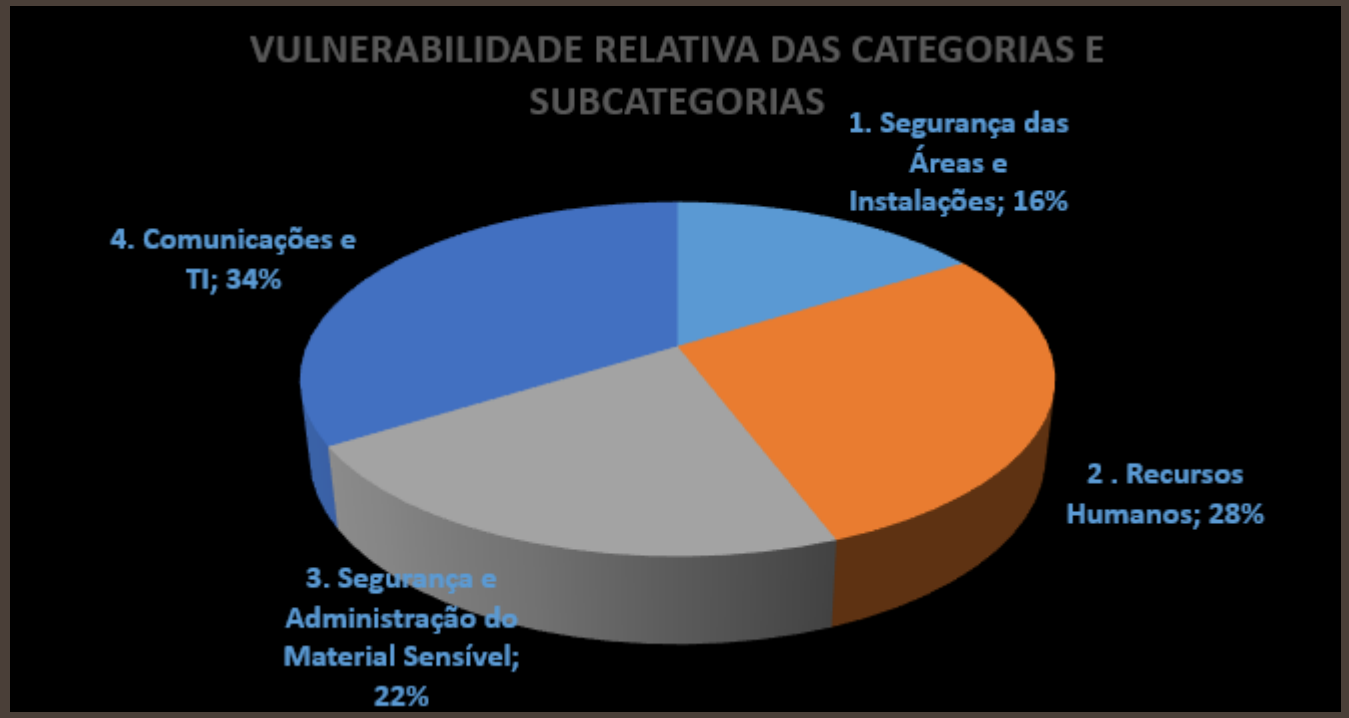
%Vulnerabilidade Total da Categoria

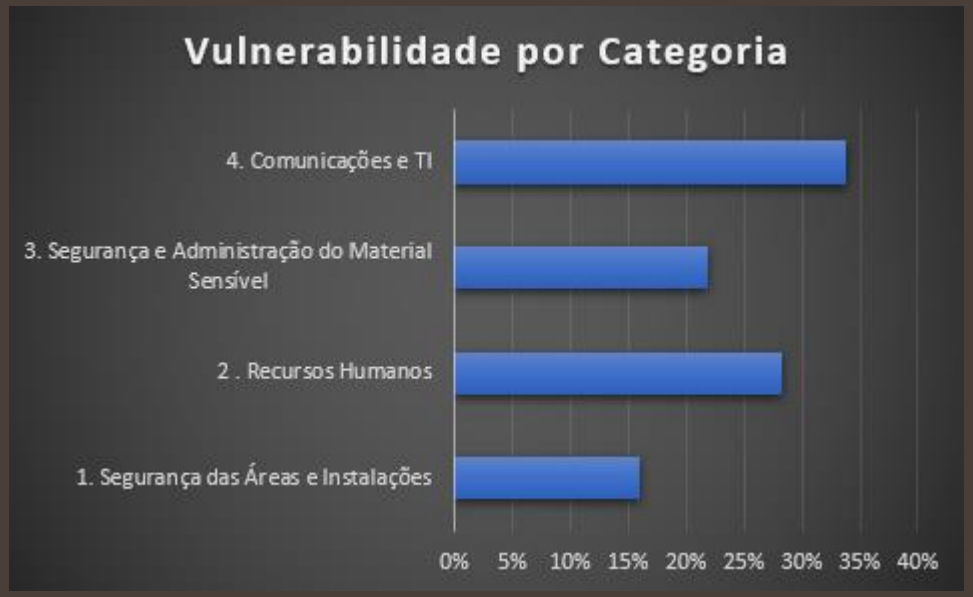
Em seguida, verificar o quanto vulnerável encontra-se o Sistema de segurança orgânica da instituição em termos percentuais, por meio do fator de vulnerabilidade.

Categoria Vulnerável	Nota	Nota Máxima	% Vulnerabilidade	% Vulnerabilidade Total
Segurança das instalações	2,09	3	34,32%	67,67%
Segurança dos Recursos Humanos	2	3	32,84%	
Segurança das Informações	2	3	32,84%	
Total	**6,09**	**9**	**100,00%**	

$$\%\text{Vulnerabilidade Sistema} = \frac{\sum \text{notas FV categorias}}{\sum \text{notas máximas}} \times 100$$

CATEGORIAS VULNERÁVEIS		NOTA DAS CATEGORIAS E SUBCATEGORIAS	VULNERABILIDADE TOTAL DA SUBCATEGORIAS	VULNERABILIDADE RELATIVA DAS CATEGORIAS E SUBCATEGORIAS	% VULNERABILIDADE TOTAL DO SISTEMA	FATOR VULNERABILIDADE DO SISTEMA
1. Segurança das Áreas e Instalações		**#DIV/0!**	**#DIV/0!**			
Subcategorias	1.1 Sistema de Barreira Física		**0,00%**	**#DIV/0!**		
	1.2 Sistema de Controle de Acesso		**0,00%**			
	1.3 Sistema de Monitoramento de Detecção Eletrônica		**0,00%**			
	1.4 Vigilância Física		**0,00%**			
	1.5 Planos de Contingência		**0,00%**			
	1.6 Área de Acesso Restrito		**0,00%**			
2 . Recursos Humanos		**#DIV/0!**	**#DIV/0!**			
Subcategorias	2.1 Supervisor de Segurança		**0,00%**	**#DIV/0!**		
	2.2 Vigilantes		**0,00%**			
	2.3 Terceirizados		**0,00%**			
	2.4 Servidores Administrativos		**0,00%**			
	2.5 Prestadores de Serviços Temporários		**0,00%**			
3. Segurança e Administração do Material Sensível		**#DIV/0!**	**#DIV/0!**			
Subcategorias	3.1 Arma / Munição / Colete balístico		**0,00%**	**#DIV/0!**		
	3.2 Crachá (Identificação)		**0,00%**			
	3.3 Sistema de Comunicação		**0,00%**			
	3.4 Chaves		**0,00%**			
	3.5 Documentação		**0,00%**			
4. Comunicações e TI		**#DIV/0!**	**#DIV/0!**			
Subcategorias	5.1 Privilégio Mínimo - Existência de autorização para		**0,00%**	**#DIV/0!**		
	5.2 Separação de funções e responsabilidades		**0,00%**			
	5.3 Recursos críticos		**0,00%**			
	5.4 Gradação de nível de criticidade		**0,00%**			
	5.5 Segurança Física		**0,00%**			
	5.6 Segurança Lógica		**0,00%**			
	5.7 Segurança do Tráfego		**0,00%**			
	5.8 Pessoal		**0,00%**			
	5.9 Administração da rede e procedimentos de segurança		**0,00%**			
	5.10 Requisitos básicos		**0,00%**			
	5.11 Estações de trabalho		**0,00%**			


VULNERABILIDADE RELATIVA DAS CATEGORIAS E SUBCATEGORIAS
1. Segurança das Áreas e Instalações; 16%
2 . Recursos Humanos; 28%
3. Segurança e Administração do Material Sensível; 22%
4. Comunicações e TI; 34%


Vulnerabilidade por Categoria
4. Comunicações e TI
3. Segurança e Administração do Material Sensível
2 . Recursos Humanos
1. Segurança das Áreas e Instalações
0% 5% 10% 15% 20% 25% 30% 35% 40%


Recursos Humanos
70,00%
60,00%
50,00%
40,00%
30,00%
20,00%
10,00%
0,00%
2.1 Supervisor de Segurança
2.2 Vigilantes
2.3 Terceirizados
2.4 Servidores Administrativos
2.5 Prestadores de Serviços Temporários

Lembrando!

Risco = PROBABILIDADE X IMPACTO

Consequências

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.

ISPS

No item 15.5, também é estabelecido que a avaliação de risco deve levar em conta a **perda potencial de vidas, a importância econômica do porto, seu valor simbólico e a presença de instalações governamentais**. Esses pontos são os parâmetros que devem ser utilizados para as consequências, e constituem **as evidências de conformidade**.

Ressalte-se aqui que esses são os parâmetros mínimos que devem constar em todo processo da avaliação de riscos para se atestar a conformidade com o ISPS Code.

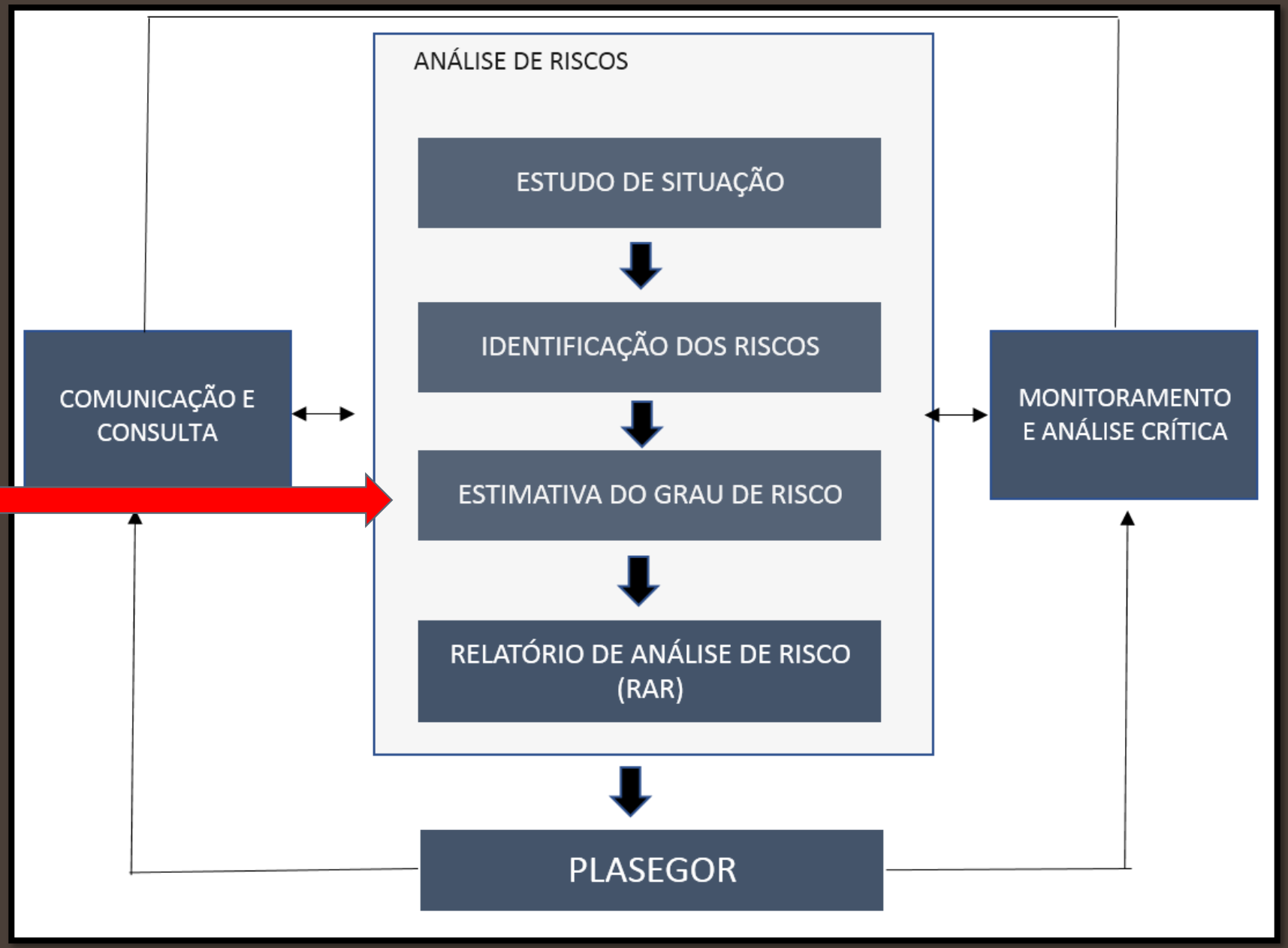
Consequências

Exemplificando: Se um método conhecido e considerado de avaliação de riscos não tiver em seu processo esses parâmetros de avaliação (a perda potencial de vidas, a importância econômica do porto, seu valor simbólico e a presença de instalações governamentais), ele não pode ser atestado como em conformidade com o ISPS Code, independentemente do argumento, por não possuir elemento caracterizador de evidência objetiva, pois estará constatado que ele não atende aos requisitos e/ou diretrizes. No caso específico, a não conformidade é o não atendimento ao item 15.5 da parte B do ISPS Code.

Consequências

IMAGEM INSTITUCIONAL			
AMEAÇA	**AÇÃO ADVERSA**	**CONSEQUÊNCIA**	**NOTA**
ORCRIM	Execução de servidores	ALTA	3
	Ameaça a servidores	MÉDIA	2
	Acesso Info. Sigilosas	ALTA	3
	Infiltração	MÉDIA	2
	Sabotagem Infra Criticas	MÉDIA	2
SERVIDORES INSATISFEITOS	Vazar Info. Sigilosas	ALTA	3
	Facilitar o acesso as A&I	MÉDIA	2
	Roubo/Furto Mat. Sens.	MÉDIA	2

CRITERIOS PARA VALORAÇAO DAS CONSEQUENCIAS		
GRAU	**NOTA**	**Descrição**
ALTA	**3**	Compromete a imagem da instituição, com impactos negativos no ambiente interno e/ou externo. Perda ou abalo da confiança na instituição. Morte, invalidez permanente, risco de vida ou necessidade de tratamento médico hospitalar emergencial. Abala consideravelmente o moral de um número significativo de membros, ocasionando a redução do ritmo e a intensidade das atividades funcionais por eles desempenhadas. Perda ou suspensão da capacidade de execução de atividades essenciais. Compromete segredos estratégicos (desestabiliza). Destruição, dano irreparável ou grave aos recursos financeiros, informacionais, materiais e/ou instalações.
MÉDIA	**2**	Ocasiona um desgaste temporário para a imagem da instituição, mas não chega a comprometer, de uma forma geral, a confiança na instituição. Não há risco de vida imediato; vítimas com necessidade de tratamento médico hospitalar não emergencial. Abala o moral de membros, sem interferir, contudo, no ritmo e intensidade das atividades funcionais por eles desempenhadas. Perda ou Suspensão da capacidade de execução de atividades secundárias (de apoio). Compromete segredos operacionais Dano significativo recuperável, mas oneroso aos recursos financeiros, materiais, informacionais e/ou instalações.
BAIXA	**1**	Não repercute sobre a Imagem da Instituição. Não influencia na confiança na instituição. Não há risco de vida imediato; vítimas com ferimentos leves tratáveis no próprio local ou sem lesões aparentes. Não afeta o moral dos membros. Interferência ou tumulto em processos internos; sem paralisação ou suspensão de qualquer atividade. Não afeta nenhum tipo de segredo institucional. Danos podem ser sanados pela manutenção orgânica.


ANÁLISE DE RISCOS
ESTUDO DE SITUAÇÃO
IDENTIFICAÇÃO DOS RISCOS
ESTIMATIVA DO GRAU DE RISCO
RELATÓRIO DE ANÁLISE DE RISCO (RAR)
COMUNICAÇÃO E CONSULTA
MONITORAMENTO E ANÁLISE CRÍTICA
PLASEGOR

Correlação dos Elementos do Risco

Risco = PROBABILIDADE X IMPACTO

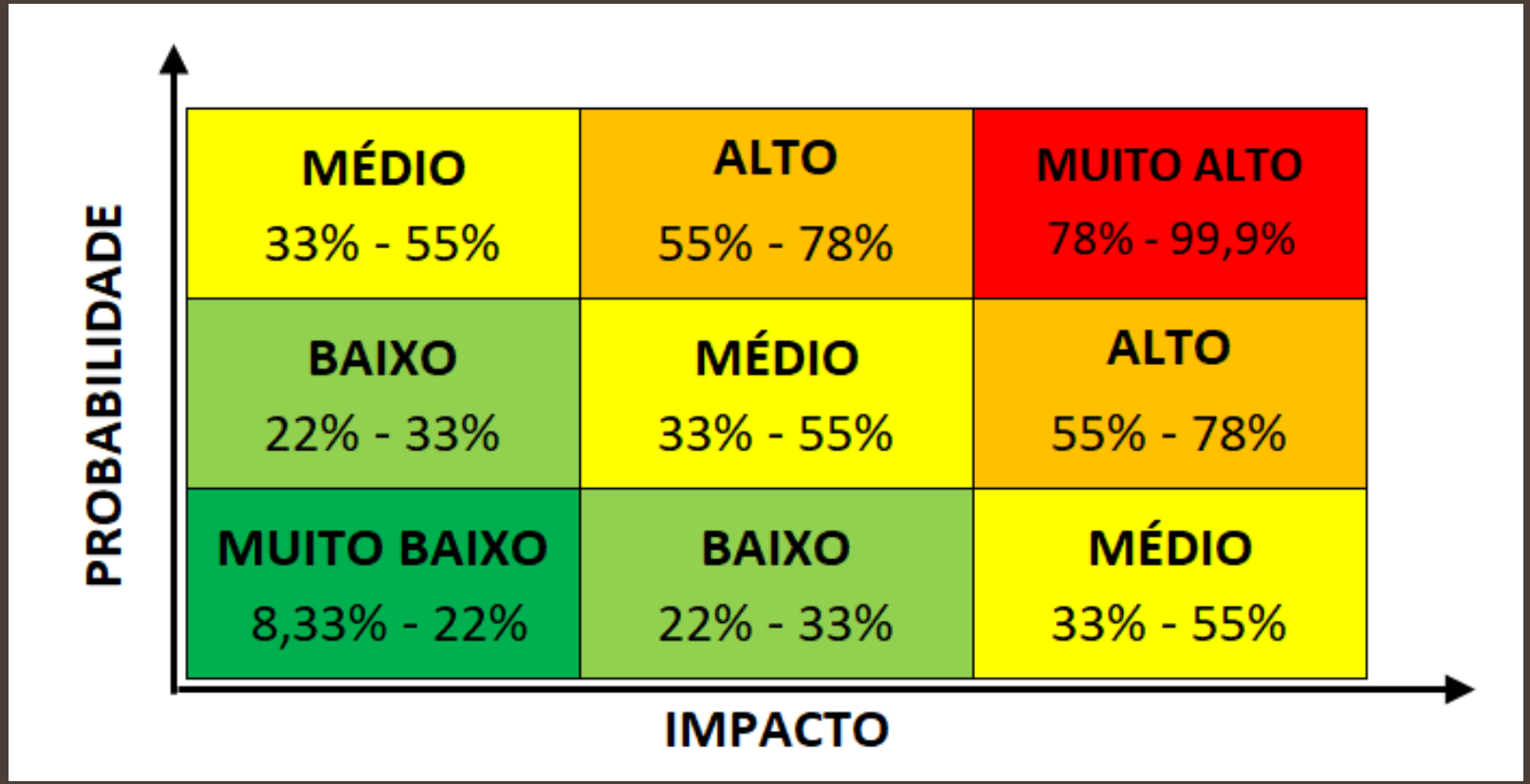
$$\text{PROBABILIDADE} = \frac{\text{Fator Vulnerabilidade} + \text{Nível de Ameaça}}{2}$$

$$\text{IMPACTO} = \frac{\text{Ativo} + \text{Consequência}}{2}$$

O grau do Risco é definido de acordo com os critérios utilizados na metodologia ARESP. Portanto, o nível do risco pode alcançar valor máximo de 9 e mínimo de 0,75, traduzindo-se em cinco possíveis estágios:

Risco - Tabela de Referência		
Classificação	Grau do Risco	
MUITO BAIXO 6,4% - 22%	0,75	1,99
BAIXO 22% - 33%	2	2,99
MÉDIO 33% - 55%	3	4,99
ALTO 55% - 78%	5	6,99
MUITO ALTO 78% - 99,9%	7	9

Matriz de Risco



Estimativa do Grau de Risco

O risco pode ser apresentado de **forma agrupada**, ou seja, com base no valor médio dos ativos, das ameaças e do fator de vulnerabilidade:

ATIVO: IMAGEM INSTITUCIONAL					
NOTA MÉDIA ATIVO	**NOTA MÉDIA AMEAÇA**	**FATOR VULNERABILIDADE**	**NOTA MÉDIA CONSEQUÊNCIA**	**RISCO**	**CLASSIFICAÇÃO**
2,5	2,3	2,03	2,6	5,556	**ALTO**

ATIVO: IMAGEM INSTITUCIONAL

PROBABILIDADE				IMPACTO				RISCO	
FATOR VULNERABILIDADE	AMEAÇA	NOTA AMEAÇA	NOTA PROBABILIDADE	AÇÃO ADVERSA	CONSEQUÊNCIA	NOTA DO ATIVO	NOTA IMPACTO	GRAU DO RISCO	CLASSIFICAÇÃO
2,03	ORCRIM	2,3	2,165	Execução de servidores	3	3	3	6,495	ALTO
		2,3	2,165	Ameaça a servidores	2		2,5	5,4125	MÉDIO
		2	2,015	Acesso Info. Sigilosas	3		3	6,045	ALTO
		3	2,515	Infiltração	2		2,5	6,2875	ALTO
		2,3	2,165	Sabotagem Infra Criticas	2		2,5	5,4125	MÉDO
	SERVIDOR INSATISFEITO	3	2,515	Vazar Info. Sigilosas	3		3	7,545	MUITO ALTO
		2	2,015	Facilitar o acesso as A&I	2		2,5	5,0375	MÉDIO
		1,6	1,815	Roubo/Furto Mat Sens	2		2,5	4,5375	MÉDIO

TRATAMENTO DO RISCO

TRATAR

Evitar o risco;

É melhor eliminar os riscos que reparar os eventuais estragos causado por eles;

ASSUMIR

Não exige nenhuma ação;

Tratamento pontual sobre o risco conforme sua ocorrencia;

MITIGAR

Requer uma atividade para reduzir, normalmente, o impacto de um risco identificado;

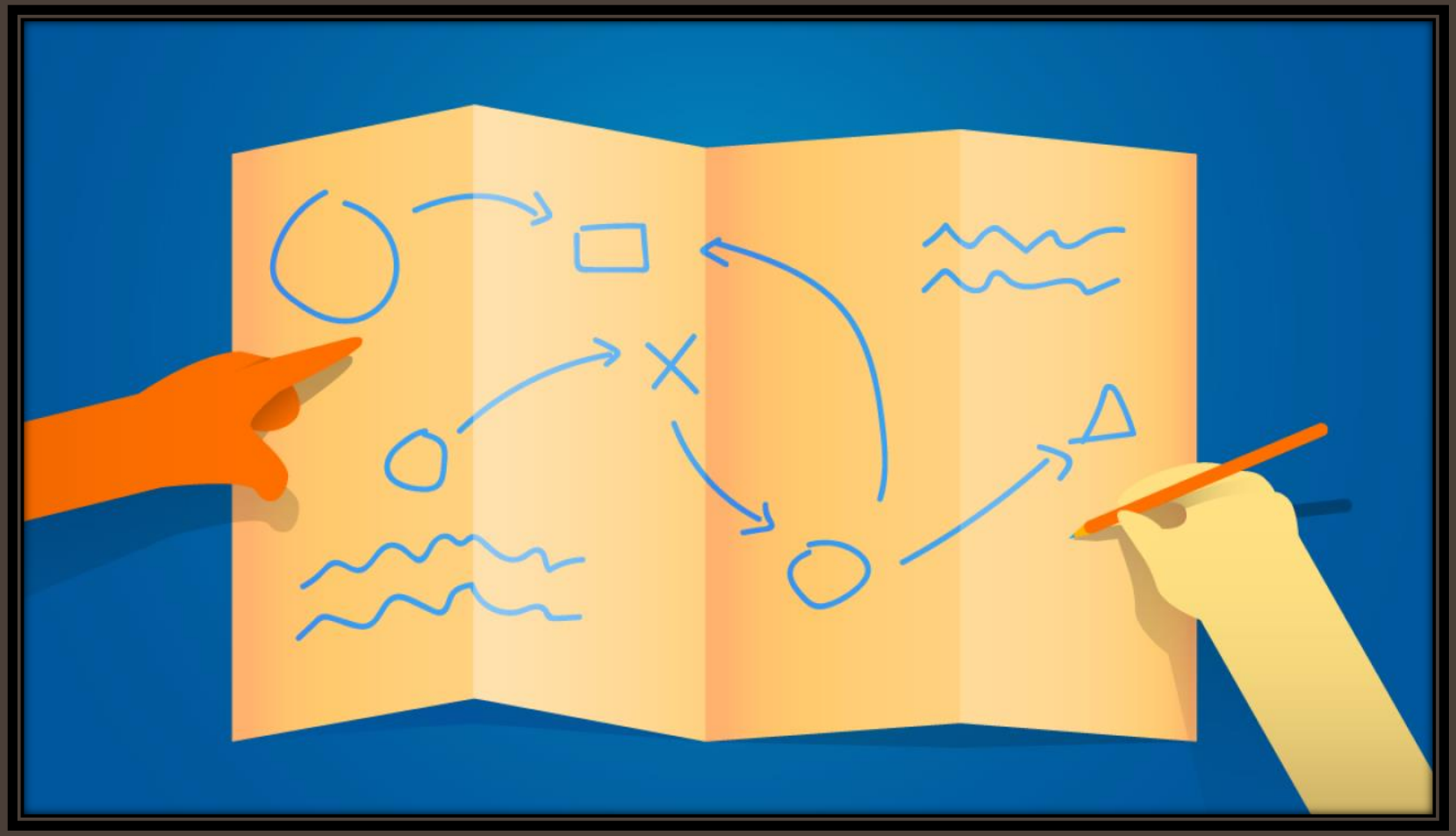
Se o risco acontecer, o custo e o impacto serão mais baixos;

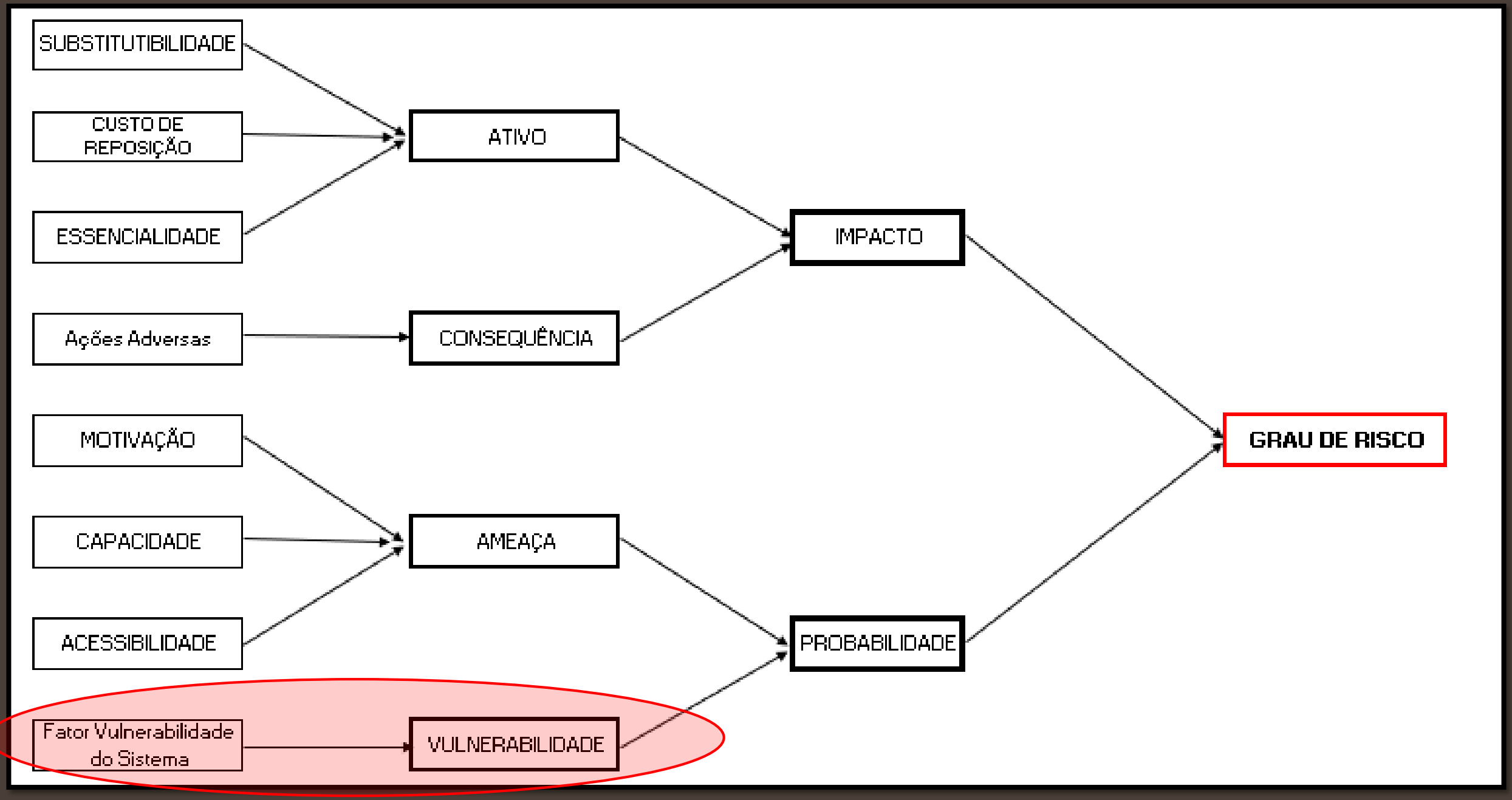
COMPARTILHAR

Transfere a responsabilidade do risco para uma terceira parte;

O risco não desaparece;

Elaboração do Plano de Segurança Portuária




SUBSTITUTIBILIDADE
CUSTO DE REPOSIÇÃO
ESSENCIALIDADE
ATIVO
IMPACTO
Ações Adversas
CONSEQUÊNCIA
MOTIVAÇÃO
CAPACIDADE
ACESSIBILIDADE
AMEAÇA
PROBABILIDADE
GRAU DE RISCO
Fator Vulnerabilidade do Sistema
VULNERABILIDADE

Considerações finais

- A metodologia ARESP já foi testada em diversos terminais portuários e está em fase de consolidação;
- A evolução do processo é contínuo e depende da aprendizagem;
- A ARESP apresenta aderência às especificidades de diversos tipos de terminais portuários;
- A metodologia é técnica, transparente, auditável e moderna;
- Atende tanto a demanda das instalações como do ISPS e Resoluções da CONPORTOS.

Fim!

Felipe Scarpelli

Scarpelli.fsa@pf.gov.br