



ISO 20 858 - Ships and marine technology — Maritime Port Facility Security Assessments and Security Plan Development

Manuel Carrasqueira Jorge Lourenço

Cofinanciado por:







Manuel Carrasqueira



PHD em Engenharia e Gestão Industrial;

Mestre em Engenharia de Materiais;

Pós-graduação em Qualidade e Gestão de Materiais;

Licenciatura em Engenharia de Máquinas.

Formação técnica e profissional nacional e internacional nos domínios da Segurança e da Proteção;

Chefe dos serviços de máquinas, manutenção e Segurança de navios da Marinha Portuguesa;

Chefe de Gabinete e Formador da Escola Segurança da Marinha Portuguesa.



Manuel Carrasqueira



- Investigador da UNL/FCT e Escola Naval;
- Membro E3 da Ordem dos Engenheiros;
- Técnico Superior acreditado pela ACT, DGRM, DGEG e Formador certificado pelo IEFP;
- Coordenador de Projectos, formador, consultor e auditor para diversas organizações nas áreas da Segurança e da Proteção;
- Expert da UE na avaliação de projectos de IDI e avaliador de projetos de IDI do Portugal 2020.



Jorge Lourenço



Doutorando em Segurança, Defesa, Relações Internacionais;

Mestre em Gestão e Comportamento Organizacional;

Pós-Graduação Análise da Ameaça Terrorista;

Licenciatura em Ciências Militares Navais – Fuzileiros.

Capitão de Mar e Guerra Marinha, Fuzileiros – Ref.

Formação técnica e profissional nacional e internacional nos domínios da *Intelligence*, Segurança e Defesa;

Formador e Consultor da NATO Special Operations School: Bélgica;



Jorge Lourenço



- Investigador do ISCTE/Instituto Universitário de Lisboa;
- Técnico Superior acreditado pelo IEFP;
- Chefe de Estado Maior do Quartel-General de Operações Especiais;
- Coordenador da
- Formador do Grupo de Operações Especiais da PSP de Macau e da Escola da Polícia Judiciária de Macau;
- Comandante do Destacamento de Acções Especiais da Marinha Portuguesa:
 - . Acções de Combate ao Narcotráfico no Mar
 - . Formação e Treino em *Maritime Counter Terrorism*



Programa da Formação



Das 10.00 às 13.00 Componente conceptual	 Contexto Internacional Importância da ISO 20858 Articulação da ISO 20858 com normas relevantes como a ISO 28000, a ISO 27001 e outras normas de gestão Principais requisitos da ISO 20858 A ISO 20858 e o código ISPS 			
	Almoço – 13.00 / 14.00			
Das 14.00 às 17.00 Componente	 Metodologia de implementação da ISO 20858 Discussão de exemplos Desenvolvimento de caso prático – trabalho coletivo 			
prático-aplicada	 Preparação do trabalho individual a desenvolver em contexto de tra lho 			





Segurança: Contexto Internacional



Segurança < > Desenvolvimento



Segurança / Proteção



Condição Básica para o Desenvolvimento e Continuidade de Negócio

Objectivo fundamental da política de Estado / Alianças / União de Estados

Finalidade > Que se pretende alcançar — Garantir liberdade de acção > continuação de um negócio sem rupturas e num ambiente controlado



Avaliação da Segurança



Transporte Marítimo & Economia Global

- 90% do comércio mundial desenvolve-se através do mar
- Complexa Rede Comercial
 - > 2010: 893.467 navios / 2018: 1.910 012 navios
 - > Cerca de **5000 portos** nos 5 continentes





Segurança e Proteção da Navegação > Medidas de Segurança à Escala Global > Consenso Internacional



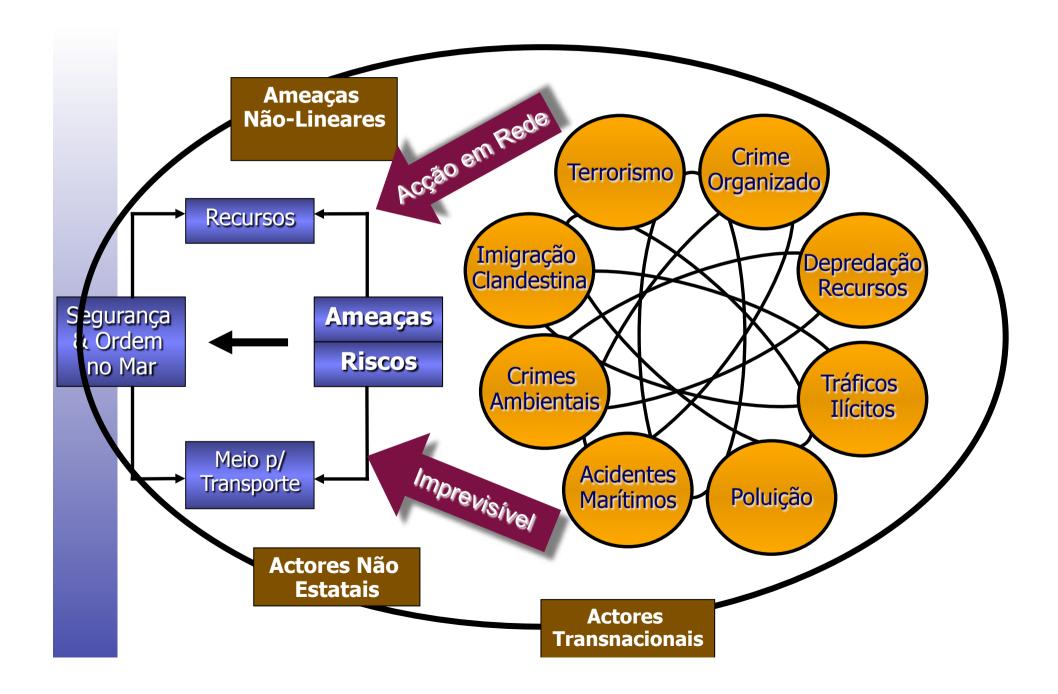


Pós 9/11

- ✓ Vulnerabilidades de segurança no sector dos transportes
 - > Ligações Globais
- ✓ Vertentes Económica, Social, Tecnológica ...
 - > Interdependência (VS) Riscos + Ameaças
- ✓ Insuficiência dos Estados > Segurança
 & Defesa > ameaças não militares











Ameaças não lineares / Terrorismo

- Dinâmicas muito fluídas / muito voláteis e interligadas à criminalidade internacional em rede podendo assumir várias formas:
 - > Ciberterrorismo,
 - Bioterrorismo, ... Armas de Destruição em Massa ...
- Crescente uso de tecnologias, técnicas e tácticas inovadoras > Imprevisibilidade
- Tira partido das vulnerabilidades e fragilidades dos estados, comunidades e organizações





Avaliação das Vulnerabilidades

Variáveis analisadas pelos Terroristas na Seleção de um Alvo:

- Acessibilidade > Como chegar ao alvo
- Prestígio > Reconhecimento e influência do alvo
- Visibilidade > Abrangência e publicitação
- Económico / Financeiro > Capacidade de exploração para obtenção de fundos e / ou recursos





Criminalidade Organizada > EX: Ciber crimes

Ciber Crime e Ciber Ataques

- Espionagem Informática
- Utilização de software malicioso malware
- Ciber ataques contra
 - Administrações Públicas
 - Organizações Privadas -Ransomware







Internet das Coisas – Machine to Machine









Drones Comerciais















Importância da ISO 20858



Importância ISO 20858



 Desenvolvida > Organização Internacional de Normalização (ISO) em consonância com o Código Internacional de Segurança de Navios e Instalações Portuárias (ISPS)



 Evidencia > Boas práticas em matéria de proteção marítimo-portuária

 A ISO 20858 constitui um eficaz suporte para o desenvolvimento e consolidação de uma cultura de segurança e proteção da IP



Importância ISO 20858



Benefícios Comerciais e de Imagem

- > Clientes que se encontram expostos a riscos significativos de segurança valorizam cada vez mais a adoção das normas ISO
- > Clientes certificados > Tendência trabalhar com fornecedores certificados > garantias que os seus processos de gestão e planificação serão facilmente compreensíveis e supervisionáveis

Benefícios na Segurança

> Dá garantias à sua Gestão de Topo e à Estrutura com responsabilidades de Gestão de Riscos, que a abordagem à segurança é feita de uma forma **sistemática e estruturada**



Importância ISO 20858



Benefícios Operacionais

- > Clara perceção dos **riscos**
- > Metodologia de abordagem dos riscos e ameaças > bem definida e consistente
- > Sustentação das medidas de proteção > **Contramedidas** para as ameaças e riscos
- > **Sustentação** da estrutura operacional de proteção



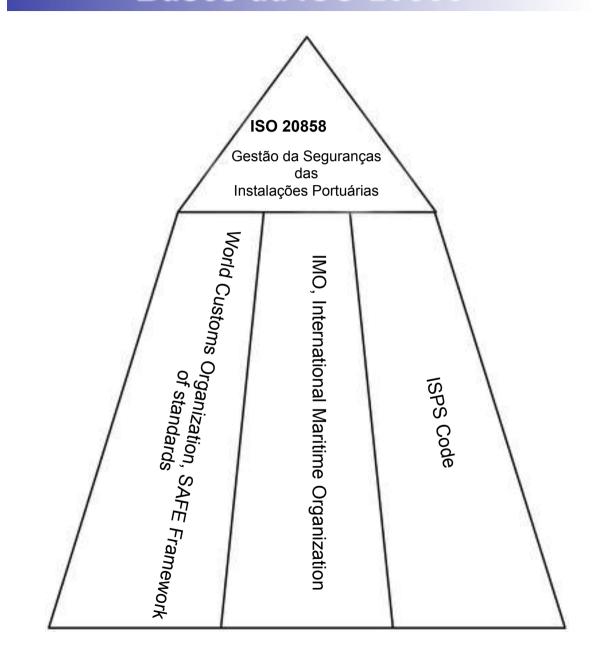


Articulação da ISO 20858 com normas relevantes: ISO 28000, ISO 27001 e outras normas de gestão



Bases da ISO 20858

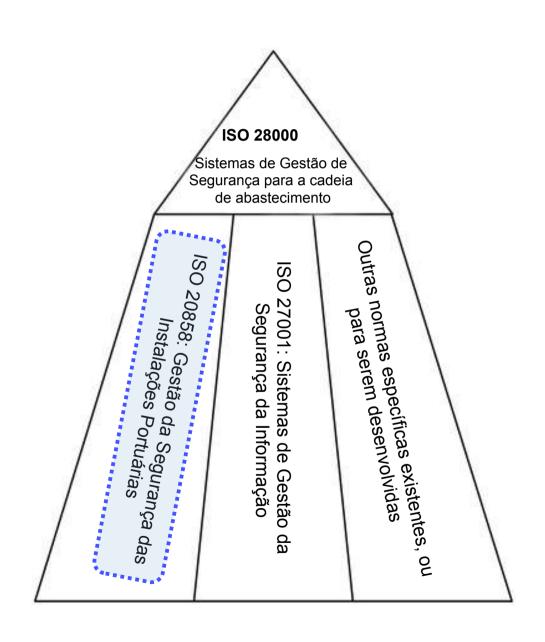






Articulação com a ISO 28000



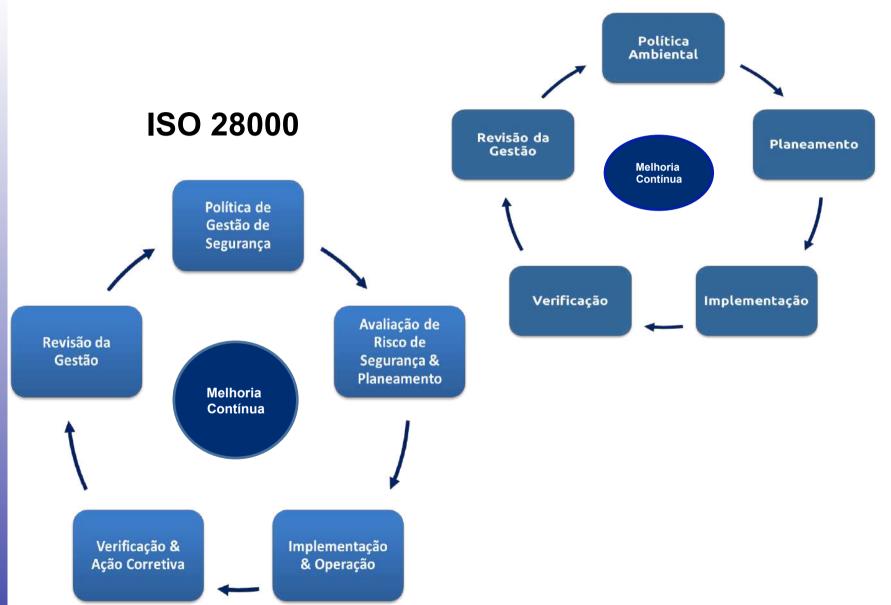




Modelo dos Sistemas de Gestão



ISO 14001

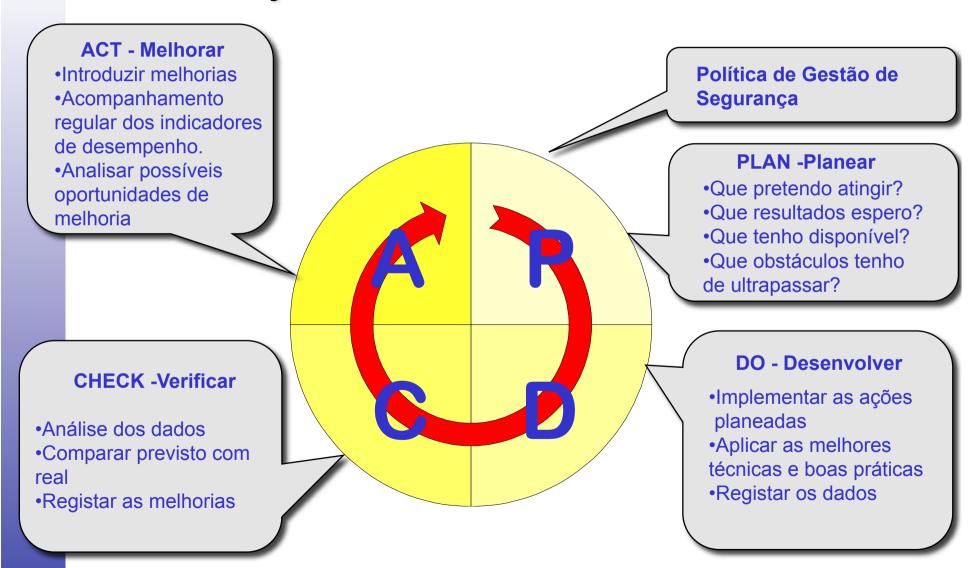




ISO 20858



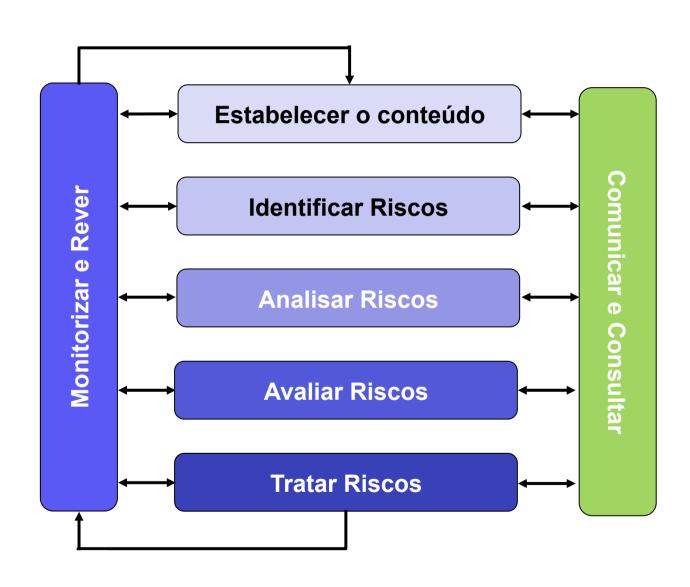
O modelo de Deming para a Gestão da Segurança das Instalações Portuárias





ISO 31000 – Gestão do Risco

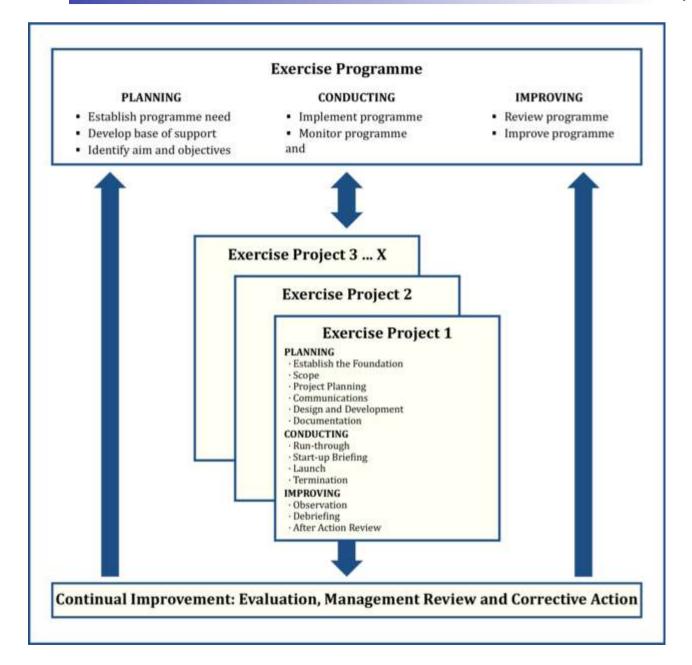






ISO 22398 – Guidelines for Exercises QUALISES







Conceitos



Alvo

Pessoal, navios, carga, **ativos** físicos, sistemas de controlo e / ou documentação dentro de uma IP.



Ameaça

Causa potencial de um incidente indesejado, que pode resultar em dano para pessoas, para um sistema ou organização, para o ambiente ou para a comunidade.





Conceitos



Carga

Itens que são colocados no navio para serem transportados para outro porto, como caixas, p unidades de transporte de carga e / ou content matérias líquidas e não líquidas a granel.



Consequência

Perda de vidas, danos à propriedade ou perturbações económicas, incluindo perturba nos sistemas de transporte que possam ser razoavelmente esperadas em resultado de u ataque na ou nas instalações portuárias.







Principais Requisitos da ISO 20858



ISO 20858



Conteúdo da norma

- ✓ Avaliação de Proteção da Instalação Portuária (APIP)
- ✓ Plano de proteção da instalação portuária (PPIP)
- ✓ Funções e competências da Estrutura de Proteção da IP





Avaliação de Proteção da Instalação Portuária - APIP

- A IP que implementa a norma > Deve basear-se numa APIP, válida documentada e que atenda aos requisitos da norma
- A APIP deve abranger
 - > Toda(s) a(s) IP(s) e infraestruturas portuárias
 - > Incluindo os **canais de navegação**, praticados pelos navios na sua de aproximação à IP







As áreas da IP

Devem ser objecto de uma **análise exaustiva e criteriosa** > requisitos de proteção

Lista de avaliação das medidas de proteção

Factores A IP dispõe documentos e procedimentos que comtemplem os aspectos seguintes?		Sim	Não	Comentários
2	A organização de segurança da IP tem ligações com as autoridades de segurança, e existe um plano de comunicações consistente e adequado às operações de proteção, ligando todos os intervenientes, incluindo os navios que se encontram na IP			







A APIP compreende

- ✓ Cenários de ameaças à segurança
- ✓ Consequências de um ataque bem sucedido
- ✓ Probabilidade de cada cenário de ameaça ser bem sucedido – e a consequente necessidade de implementar medidas de proteção > Contramedidas

São definidas contramedidas para os cenários com valorizações média e alta tanto em probabilidade como em consequência



ISO 20858



- A APIP compreende
 - ✓ Descrição das contramedidas em função das vulnerabilidades identificadas

✓ Avaliação das contramedidas



ISO 20858



Plano de Proteção da Instalação Portuária - PPIP

- Visão Geral > Repositório completo e rigoroso da descrição do funcionamento da segurança da IP
 - > Visa a **proteção**
 - ✓ Pessoal
 - ✓ Infraestrutura
 - ✓ Navios atracados
 - ✓ Carga / Unidades de Transporte de Carga
 - ✓ Sobressalentes dos navios que demandam a IP





- Deve abranger os perímetros e áreas consideradas na APIP, bem como:
 - > Todas as portas e pontos de acesso
 - > Áreas restritas nas IPs
 - > Cais e / ou pontões de atracação de navios e embarcações
 - > Equipamentos de emergência
 - > Áreas de estacionamento
 - > Portarias e postos de controlo de acessos à IP
 - > Edifícios da IP
 - > Fluxos de tráfego, incluindo faixas de veículos de emergência
 - > Áreas de armazenamento de materiais perigosos
 - > Infraestruturas críticas dentro da IP







- Tem por base os cenários e as contramedidas identificadas na APIP
- Definição e aplicação dos Níveis de Proteção notificação de navios a cais, a entrar ou a largar da IP, quando houver um aumento no nível de proteção
 - > Nível 1 > Normal: O nível em que a IP opera normalmente
 - > Nível 2 > **Reforçado**: Quando existir um risco acrescido de Incidente de Proteção
 - > Nível 3 > **Excecional**: Nível aplicável pelo período em que é provável ou iminente a ocorrência de Incidente de Proteção





Plano de Proteção da Instalação Portuária - PPIP

- Define e Descreve > Procedimentos
 - > Interface com os navios > em todos os níveis de segurança
 - Adicionais para IPs que recebem navios de passageiros
 e Ferry Boats em todos os níveis de proteção
 - > Sistema de **Comunicações** Interno e Externo > Redundâncias > medidas possam ser implementadas com rapidez e eficiência
 - > Equipamentos de Proteção
 - ✓ Inspeções
- ✓ Registo de Avarias
- ✓ Calibrações
 - ✓ Reparação

✓ Planos de Manutenção





Plano de Proteção da Instalação Portuária - PPIP

- Procedimentos > Controlo de Acessos
 - > Contra introdução de **substâncias perigosas** e **dispositivos perigosos**
 - > **Autorizações** / Cartões de Acesso
 - > Verificação
 - √ Bagagens
 - ✓ Bens e Fornecimentos

Dispositivos de Segurança





- Controlo de Acessos > Áreas Restritas
 - > Condições para acesso
 - > Registo: Pessoas / Cargas / Descargas outras manobras / operações
 - > Para o Acesso > **Medidas de Coordenação**
 - ✓ Transportadores
 - √ Fornecedores
 - ✓ Prestadores de Serviços
 - > Medidas Adicionais > Níveis de Proteção 2 e 3





- Medidas e Requisitos Adicionais de Proteção
 - > IP's que recebem navios de passageiros e ferry boats
 - > Específicas para **Terminais de Cruzeiros**
 - > Para entrega de carga destinada a **armazéns de apoio** aos navios na IP
 - > Vigilância da IP > Lado de Terra e de Mar
 - > Em Incidentes de Proteção
 - > Auditorias e Alterações ao PPIP
 - > Salvaguarda e Arquivo: **Documentação** > Relatórios e Registos





- Especifica a Estrutura de Proteção da IP e as respectivas responsabilidades
 - > Gestão da Proteção
 - > Oficial de Proteção da IP OPIP
 - > Pessoal de Proteção
 - > Pessoal que manuseia e / ou tem acesso à documentação relacionada a cargas ou provisões de navios
 - > Pessoal subcontratado a empresas de segurança privadas e tenha para funções de proteção na IP





- Estrutura de Proteção da IP > O PPIP > Base
 - > A **formação** dos colaboradores
 - > Desenvolvimento de **treinos e exercícios**
 - > Consolidação de **processos** e automatismos
 - > Verificação da **adequabilidade** dos procedimentos
 - Validação de requisitos adicionais de segurança –
 Níveis de Proteção 2 e 3
 - > Especificação de **medidas para interface** com os navios
 - > Clarificação das **comunicações** internas e externas à IP > Forças de Segurança, outras





A ISO 20858 e o código ISPS



A ISO 20858 e o código ISPS



- Concebida para assegurar o cumprimento dos requisitos da IMO relativamente à segurança marítimo-portuária, vertidos no código ISPS
- O âmbito centra-se nas Instalações Portuárias (I.P.);
- Enquanto o código ISPS é de cumprimento mandatório para todos os países signatários, a ISO 20858 é de emprego voluntário
- Define Boas Práticas para a realização da APIP e do PPIP, bem como disponibiliza um checklist abrangente à totalidade dos requisitos de Proteção/Security aplicáveis a uma I.P.



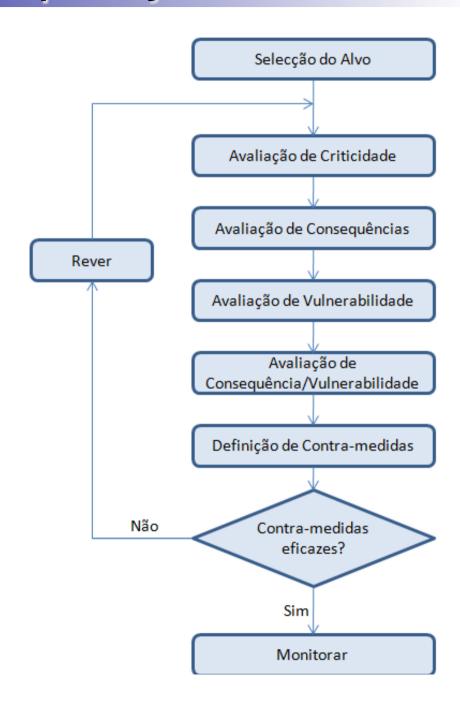


Metodologia de implementação da ISO 20858



Apreciação do Risco







Criticidade dos Alvos



Avaliação da criticidade dos alvos

Alvo	Atividade	Efeitos no Alvo	Recup.	Criticidade
Portaria	Segurança e controlo de acessos	Perda de vidas Efeitos psicológicos Segurança pública	Boa	Moderada
Edifícios e instalações	Administrativas, produtivas e de suporte	Perda de vidas Impacto económico Efeitos psicológicos	Boa	Moderada



Consequências



Classificação de Consequências – Exemplo

ALTAS

- Perda de vidas em grande escala
- Danos a infraestruturas que impedem operações futuras
- Destruição total de um ecossistema

MÉDIAS

- Perda de vidas em certa escala
- Danos a ativos ou infraestruturas que requerem reparação
- Danos a largo prazo de partes de um ecossistema

BAIXAS

- Lesões sem perda de vidas
- Danos menores a ativos ou infraestrutura
- Danos ocasionais



Categoria e Grau da Vulnerabilidade QUALISES



Categoria Grau	Disponibilidade	Acessibilidade	Organização de Proteção	Resistência do alvo
Elevado	Sempre disponível De presença contínua De presença regular	Sem obstáculos nem restrições à entrada ou movimentação no seu interior	Sem qualquer tipo de organização de proteção (planos contingência comunicações , etc.)	Facilidade em danificar ou destruir o alvo
Médio	Disponível com frequência Horário previsto com antecedência	Boa capacidade de deteção Obstáculos à entrada e na proximidade	Boa organização de proteção (Planos, sistemas, deteção)	Construção robusta do alvo
Baixo	Raramente disponível Sem escala previsível e conhecida	Grande capacidade de deteção Acessos limitados Várias barreiras	Excelente organização de proteção sob todos os aspetos	O alvo pode conter o ataque



Avaliação da Vulnerabilidade



Disponibilidade	A existência e presença do alvo, a sua exposição e grau de probabilidade de sofrer um ataque
Acessibilidade	Condições de acesso para um ataque ao alvo, considerando a existência (ou não) de barreiras físicas/geográficas para conter uma ameaça sem recurso a medidas de proteção
Organização de Proteção	Capacidade do sistema e do pessoal de proteção em deter um ataque. Inclui planos de contingência, capacidade de comunicação, sistemas de deteção, etc.
Resistência	Capacidade do alvo em conter, por si só, um ataque. Considerar a complexidade do alvo, a sua conceção e as características dos materiais usados



Avaliação da Probabilidade



CLASSIFICAÇÃO	CRITÉRIOS
Baixa	Medidas implementadas oferecem resistência substancial
Média	Medidas implementadas oferecem resistência moderada
Alta	Medidas implementadas oferecem baixa resistência



Avaliação do Risco



Vulnerabilidade		Nula	Pouca	Média	Alta
Impacto	1	2	3	4	
Local/Confiança	1	1	2	3	4
Material / Bens	2	2	4	6	8
Económico / Ambiental	3	3	6	9	12
Segurança Nacional	4	4	8	12	16
Perdas Humanas	5	5	10	15	20



Capacidade de Recuperação



Capacidade de recuperação					
Nenhuma	Recuperação pode ser inviável ou superior a 1 ano				
Deficiente	Recuperação pode significar vários meses				
Fraca	Recuperação em poucos meses				
Воа	Recuperação na escala das semanas				
Excelente	Recuperação quase imediata ou na escala dos dias				



Seleção dos Cenários



Seleção dos cenários							
Alvo / Cenários	Objetivos	Motivações	Meios				
Edifícios e instalações Colocação de explosivos Veículo armadilhado Incêndio / Explosão / Destruição	Destruir / danificar Eliminar / reduzir capacidade controlo	Económicas Político-sociais Psicológicas	Acesso por água ou terra Explosivos Veículo Ativação de incêndio				



Análise Vulnerabilidade / Consequência



Grau de	Grau de Vulnerabilidade				
Consequência	Baixo	Médio	Elevado		
Consequencia	Ação				
Elevado	Considerar	Conter	Conter		
Médio	Documentar	Considerar	Conter		
Baixo	Documentar	Documentar	Considerar		



Quando definir Contramedidas QUALISES



			CONSEQUÊNCIA	
	X 20	Alta	Média	Baixa
	Alta	Contramedidas	Contramedidas	
PROBABILIDADE	Média	Contramedidas	11	
	Baixa			



Ação por cenário



Alvo	Cenário de Ameaça	Grau de Criticidade	Grau de Consequência	Grau de Vulnerabilidade	Ação
Infraestruturas e Instalações, incluindo Cais e	Incêndio / Explosão/Destruição	Crítico	Elevado	Médio	Conter
Tanques Armazenagem	Atividades ilícitas		Baixo	Médio	Documentar





Discussão



Ameaças



Como encara os atuais fluxos de Migração

 Desenvolva uma avaliação de prós e contras em termos de ameaças de Terrorismo, no curto e no médio / longo prazos



Ameaças



- Sendo Ameaça a resultante da Probabilidade/ Frequência pela Severidade/Consequência, ordene por prioridade as seguintes tipologias de medidas?
 - > As que visam reduzir a Probabilidade
 - > As que visam reduzir a Consequência
 - > As que visam reduzir simultaneamente a Probabilidade e a Consequência



Pessoal



 Será razoável / possível solicitar info detalhada do pessoal de um fornecedor, como Registo Criminal?



Funções e Responsabilidades



 Avalie a razoabilidade das 3 medidas abaixo para os diferentes níveis de proteção.

Madidas de Dustassão	Nível de Protecção			
Medidas de Protecção	1	2	3	
Todo o pessoal do porto deverá rever e exercitar os seus deveres e responsabilidades, através da execução de treinos e exercícios.	V	1	¥	
Disponibilizar informação de protecção a todo o pessoal a quem se destine a alteração do nível de protecção e qualquer informação específica de ameaça.	Opcional	1	1	
O Oficial de Protecção comunicará com o navio coordenando medidas de protecção.	1	1	4	





Desenvolvimento de Casos



Auto-avaliação



 Selecione uma Instalação Portuária que, expectavelmente, estará no âmbito da implementação e certificação pela ISO 20858

 Proceda à autoavaliação da conformidade da situação atual da I.P., face aos requisitos da ISO 20858 utilizando para tanto o check-list da norma?



Apreciação do Risco



 Identifique os 3 alvos mais relevantes da sua entidade;

 Proceda à Apreciação do Risco, seguindo a metodologia definida até ao estabelecimento de Contramedidas;

 Em articulação com o OPIP da Instalação Portuária considerada, avalie eventuais desalinhamentos face à documentação em vigor (APIP e PPIP) identificando os principais impactes decorrentes da apreciação efetuada.





QUESTÕES?