QUALIseg
ENGENEERING AND MANAGEMENT

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

Gestão da Segurança das Instalações Portuárias (SGIP)

Projecto:

GISAMP

Cofinanciado por:

REPÚBLICA PORTUGUESA
MAR

fundoazul

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

Índice

1. Introdução à norma ISO 20858 4

2. Benefícios da implementação da norma ISO 20858 5

- Comercial/Imagem 6
- Garantia de Segurança 6
- Operações 6

3. Principais conceitos e terminologia 7

4. Pensamento baseado no Risco 10

5. Ciclo PDCA 11

6. Metodologia de implementação 12

7. Gestão Integrada 14

8. Cláusulas normativas da ISO 20858 16

Generalidades 16

Desenvolvimento da Avaliação de Proteção da Instalação Portuária (APIP) 17

- Visão Geral da Avaliação de Proteção 17
- Pessoal que conduz a APIP 17
- Âmbito do desenvolvimento da APIP 18
- Contactos com Forças e Serviços de Segurança do Estado (FSSE) 19
- Avaliação de consequências 19
- Classificação da Probabilidade da Ocorrência de Cenários de Proteção 19
- Contramedidas 20

Plano de Proteção da Instalação Portuária (PPIP) 20

- Visão geral do PPIP 20
- Âmbito do desenvolvimento do PPIP 21
- Estrutura Funcional de Proteção da IP 22
- Alterações nos níveis de proteção 22
- Procedimentos de interface com os navios 22
- Declaração de Proteção (DoS – Declaration of Security) 22
- Requisitos adicionais para instalações portuárias que recebem navios de passageiros no Nível de Proteção 1 22
- Comunicações 23
- Manutenção dos Equipamentos de Proteção 23
- Medidas de proteção para controle de acesso, incluindo áreas de acesso público 24
- Medidas de proteção para áreas restritas 24
- Acesso a áreas restritas 24
- Medidas de proteção para entrega de carga destinada a armazéns de apoio aos navios na IP 24
- Medidas de proteção de vigilância da IP 25
- Procedimentos em incidentes de segurança / proteção 25
- Requisitos adicionais para instalações de passageiros e ferry boats 25
- Requisitos adicionais em terminais de cruzeiros 26
- Auditorias e alterações ao PPIP 26
- Treinos e exercícios 26
- Execução do plano de segurança da cadeia de abastecimento 27
- Documentação 27

9. Certificação 28

10. Referências 29

1

Introdução à norma ISO 20858

Esta Norma internacional, foi desenvolvida pela Organização Internacional de Normalização (ISO), trata da execução de avaliações de proteção da instalação portuária (APIP) e de planos de proteção da instalação portuária (PPIP), bem como das funções e competências exigíveis aos colaboradores da instalação portuária (IP) no âmbito da proteção.

A norma foi concebida em consonância com o Código Internacional de Segurança de Navios e Instalações Portuárias (ISPS), relevando as boas práticas em matéria de segurança marítimo-portuária e permitido a verificação da sua conformidade por auditores externos à IP, nomeadamente por organizações de proteção devidamente credenciadas.

Adicionalmente, a norma estabelece requisitos da documentação e evidencia os processos para a execução das tarefas acima mencionadas, permitindo a sua verificação por parte de uma organização devidamente credenciada para o efeito. No caso de Portugal, a credenciação das organizações de proteção reconhecidas para Instalações Portuárias e para Navios é conferida pela Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM), organismo público que tutela o desenvolvimento da segurança e dos serviços marítimos, incluindo o sector marítimo-portuário.

A gestão de topo da IP deve patentear a sua atenção e manifestar a sua exigência no cumprimento das normas e requisitos de proteção da IP, pelos diferentes níveis hierárquicos da organização, apreciando designadamente a avaliação contínua das vulnerabilidades, riscos, e ameaças à proteção da IP.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

2

Benefícios da implementação da norma ISO 20858

A adequada gestão da segurança e proteção das IP é vital para a o eficaz e eficiente funcionamento das mesmas. Uma IP só consegue operar se estiver garantida a sua proteção contra riscos, desafios e ameaças à sua integridade e à sua operação.

A planificação e gestão das IP tendo por base o referencial ISO 20858 facilita a implementação das boas práticas para uma gestão mais eficiente dos requisitos do código ISPS, revelando-se igualmente fulcral para a actividade da IP. Mais 90% dos bens transacionados à escala global são transportados por via marítima. O transporte marítimo é, pois, absolutamente fulcral para o funcionamento da economia mundial, para o desenvolvimento dos estados e das respectivas economias, e, é na sua essência sistémico e interdependente, pelo que a segurança e proteção da navegação e das IP se revela como uma preocupação universal, carecendo de apoio e consenso internacional.

As soluções nacionais ou ações governamentais unilaterais, só por si, revelam-se insuficientes. A norma ISO 20858 é um padrão de requisitos destinada a ajudar a gestão das IP a planificar e implementar processos de segurança e proteção em conformidade com regulamentos da Organização Marítima Internacional (IMO - International Maritime Organization) e com os requisitos do código ISPS, adoptados por uma multiplicidade de estados.

Assim, a implementação de um Sistema de Gestão de Segurança da IP e a sua certificação segundo a ISO 20858, quando realizada de forma eficaz e eficiente, traz vários benefícios, designadamente os que seguidamente se descrevem seguidamente.

2 Benefícios da implementação da **norma ISO 20858**

Comercial/Imagem

- O facto de uma organização ter um Sistema de Gestão certificado por uma entidade certificadora - externa e independente da organização – oferece uma vantagem competitiva imediata.

- Clientes que se encontram expostos a riscos significativos de segurança valorizam cada vez mais a adopção das normas ISO, bem como clientes já certificados têm como tendência trabalhar com fornecedores com a mesma certificação, tendo assim garantias que os seus processos de gestão e planificação serão facilmente compreensíveis e supervisionáveis.

Garantia de Segurança

Possuir um Sistema de Gestão devidamente robusto e implementado dá garantias à sua Gestão de Topo, bem como à restante estrutura com responsabilidades de gestão de riscos, que a abordagem à segurança é feita de uma forma sistemática e estruturada. A ISO 20858 é a norma internacionalmente reconhecida para a implementação de um Sistema de Gestão da Segurança da IP, garantindo com a sua certificação a validação por uma equipa independente.

Operações

A ISO 20858 dá suporte ao desenvolvimento de uma cultura interna na organização onde a percepção dos riscos de segurança é valorizada e a metodologia para os tratar está bem definida e é aplicada de forma consistente.

Essa consistência na abordagem leva a que o custo – seja financeiro ou de esforço – para a implementação de novos controlos, bem como a revisão dos existentes, seja cada vez menor, tal como as consequências de uma falha de segurança serão minimizadas e mais facilmente mitigadas.

3 Principais conceitos e terminologia

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.

Armazéns de apoio ao navio
Estruturas na IP que permitem armazenar mercadorias, e / ou sobressalentes a serem carregadas ou descarregadas de um navio que demande a IP.

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

Cenário de Ameaça à Protecção
Meios pelos quais um possível incidente de segurança pode ocorrer.

OBSERVAÇÃO \\ Como os métodos de ataque são quase infinitos, vários cenários gerais de ameaças à segurança são especificados para abordar toda a gama de cenários de ataques. A avaliação de proteção pode adicionar cenários de ameaças à proteção e segurança mais específicos à lista de cenários gerais de ameaças que possam afectar a integridade e proteção da IP, dependendo das circunstâncias locais.

Código Internacional de Segurança de Navios e Instalações Portuárias
(ISPS - *International Ships and Port Facility Security Code)*

Prescreve responsabilidades atribuíveis aos governos dos países, empresas de transporte marítimo, pessoal de bordo, e pessoal das IP em matéria de proteção, visando garantir a proteção do transporte marítimo e da instalação portuária contra ameaças e actos ilícitos intencionais. O Código é composto pela Parte A (cujas disposições serão tratadas como obrigatórias), e pela Parte B (cujas disposições são tratadas como recomendatórias), tal como adotado em 12 de dezembro de 2002 pela Resolução 2 da Conferência dos Governos Contratantes da Convenção Internacional para a Segurança no Mar de 1974 (Convenção SOLAS – Safe of Life at Sea).

3 Principais conceitos e terminologia

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

Declaração de Proteção - DoS
É um acordo conseguido entre um navio e ou uma IP ou outro navio com o qual interage, que providencia meios para assegurar que as responsabilidades críticas de proteção estão devidamente atribuídas, e que a proteção permanecerá assegurada enquanto durar o interface do navio com a IP ou com o outro navio.

Equipe de gestão de crise de proteção
Grupo de pessoas que têm o conhecimento / **capacidade** e autoridade para trazer os recursos necessários / **mobilizar os recursos** necessários para o caso de uma ameaça de segurança iminente ou incidente de segurança real.

Incidente de Proteção
Acto suspeito ou circunstância que ameaça a segurança de um navio ou IP.

Instalação Portuária (IP)
Área(s) do porto em que tem lugar a interface navio / porto. Inclui, consoante adequado, os fundeadouros, os cais de espera e os acessos pelo lado do mar;

OBSERVAÇÃO \\ A interface navio / porto patenteia as interações que ocorrem quando um navio é direta e imediatamente afetado por ações que envolvem o movimento de pessoas e / ou mercadorias, ou as provisões de serviços portuários de e para o navio. Para além de as referidas interações ocorrem no porto propriamente dito, podem ainda ocorrer noutras áreas como cais ou pontes de atracação ou cais de espera da IP. A IP estende-se para terra até ao limite do seu perímetro de segurança. Note que, para os fins desta Norma Internacional, pode haver mais de uma instalação portuária num porto. Caso de terminais de carga e descarga específicos das cargas a embarcar ou desembarcar. Pode haver IP e portos que são abordados no Código ISPS, mas que não são abordados nesta Norma.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

3 Principais conceitos e terminologia

Nível de Proteção
Significa a definição de um grau de risco, tendo em conta a possibilidade de um incidente de proteção poder ocorrer ou ser tentado.

Nível 1 de Proteção
Nível de proteção em que devem vigorar permanentemente medidas de proteção mínimas adequadas. Constitui o nível em que a IP normalmente opera.

Nível 2 de Proteção
Nível de proteção em que devem vigorar durante um determinado período medidas de proteção adicionais adequadas devido a risco acrescido de incidente de proteção.

Nível 3 de Proteção
Nível de proteção em que devem vigorar durante um período limitado medidas de proteção suplementares especiais, devido à probabilidade ou iminência de um incidente de proteção, mesmo que não seja possível identificar o alvo.

Oficial de Proteção da Companhia – OPC
Pessoa designada pela Companhia proprietária do(s) navio(s) para assegurar que é feita uma Avaliação de Riscos do Navio, que é elaborado um Plano de Proteção do Navio, submetido a aprovação depois do que é implementado e mantido, e para contacto com os Oficiais de Proteção das Instalações Portuárias (OPIP) e com os Oficiais de Proteção dos Navios (OPN).

Oficial de proteção da Instalação Portuária – OPIP
Pessoa Designada como responsável pela elaboração, aplicação, revisão e manutenção do Plano de Proteção da Instalação Portuária (PPIP).

Oficial de Proteção do Navio – OPN
Pessoa a bordo de um navio, respondendo perante o Comandante, designada pela Companhia proprietária do navio como responsável pela Proteção do Navio, incluindo a manutenção e implementação do PPIP, e pelos contactos com o Oficial de Proteção da Companhia e com os Oficiais de Proteção das Instalações Portuárias (OPIP) Organização Marítima Internacional (IMO - International Maritime Organization) Agência especializada das Nações Unidas cujo propósito é "fornecer mecanismos para a cooperação entre governos no âmbito da regulamentação e procedimentos técnicos atinentes ao transporte marítimo; encorajar e facilitar a adoção de normas relativas à segurança marítima, eficiência da navegação e prevenção e controle da poluição marítima causada por navios".

Pessoal de Proteção (Equipe de Proteção)
Indivíduos a quem estejam atribuídas funções de segurança e proteção definidas na IP, e, que possam, ou não, ser colaboradores.

Plano de Proteção da Instalação Portuária (PPIP)
Documento que agrega o repositório completo e rigoroso da descrição do funcionamento da segurança da IP, elencando as medidas destinadas a proteger as pessoas, as IP, navios, cargas, as unidades de transporte de carga (e/ou contentores) e as instalações de apoio aos navios dentro das IP, contra os riscos de incidentes de proteção.

Probabilidade de ocorrência
Possibilidade de um cenário de ameaça se tornar num incidente de segurança, considerando a robustez das medidas de segurança física e operacional em vigor na IP.

Protecção
Resistência a ato(s) intencional(ais), não autorizado(s), destinado(s) a causar prejuízo ou dano em navios e IP.

Risco
Possibilidade da ocorrência de danos, avarias ou perdas prováveis como consequência de uma ameaça e a probabilidade de sua ocorrência.

Sistema de Gestão
Conjunto de elementos e processos interligados e integrados na estrutura de uma organização com o objectivo de estabelecer políticas, dirigir os processos organizacionais e administrar os seus recursos e activos com vista ao cumprimento dos objectivos da organização.

4

Pensamento baseado no Risco

O risco é inerente a todos os aspectos dos Sistemas de Gestão. O pensamento baseado no risco assegura que estes riscos são identificados, considerados e controlados ao longo de toda a cadeia de processos do sistema.

A abordagem do pensamento baseado em risco define que as atividades de uma organização compreendidas no âmbito do Sistema de Gestão, deverão ser avaliadas tendo em conta a incerteza inerente ao resultado esperado. Ou seja, o impacto de cada atividade e o seu risco anexo deverão ser tidos em conta, tornando-se assim uma ferramenta para as decisões de gestão.

Em edições anteriores das normas de Sistemas de Gestão ISO, as cláusulas existentes sobre ações preventivas estavam separadas do todo. Ao usar o pensamento baseado no risco, a consideração a realizar sobre os riscos e os seus impactos é integral e deverá ser considerada em todas as fases do Sistema de Gestão, tornando-se assim proativa na prevenção, mitigação ou redução dos efeitos indesejáveis, através de uma identificação no início da cadeia, bem como nas suas ações.

Sendo assim, o pensamento baseado no risco deverá ser uma constante em todas as fases inerentes às actividades de planeamento, operação, análise e avaliação do Sistema de Gestão.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

5

Ciclo PDCA

As normas ISO de Sistemas de Gestão seguem o ciclo PDCA, também chamado ciclo de Deming. O ciclo PDCA é composto pelas componentes “Plan-Do-Check-Act” (Planeamento, Operação, Análise e Melhoria).

De uma forma sequencial, estas componentes podem ser descritas na seguinte forma simples:

1. Plan (Planeamento)

Estabelecer objectivos, recursos necessários, requisitos das partes interessadas, políticas organizacionais e identificar risco e oportunidades.

2. Do (Operação)

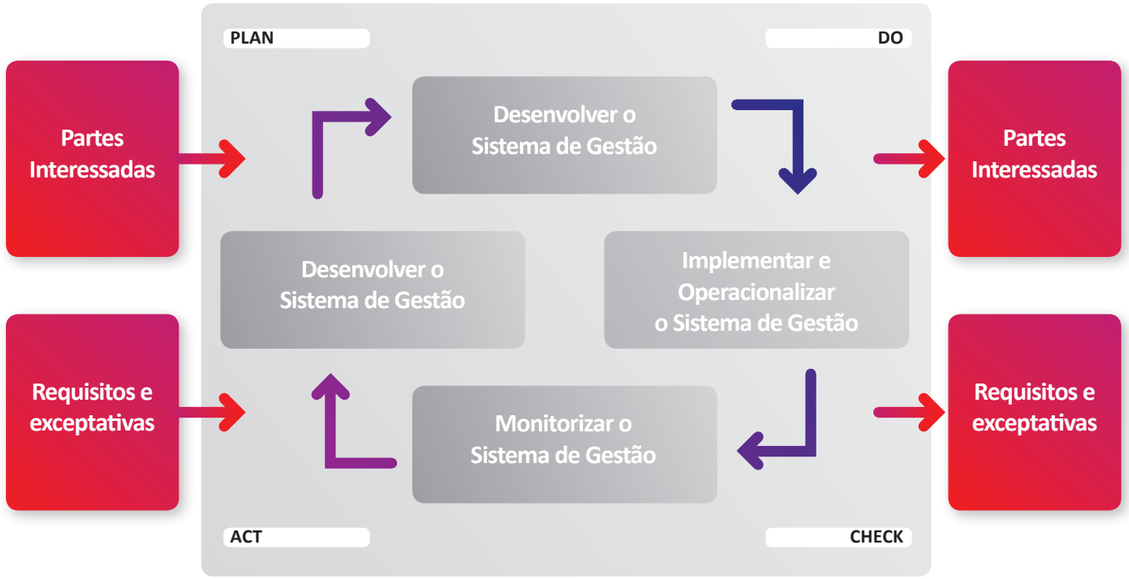
Implementar as ações planeadas.

3. Check (Análise)

Monitorizar e medir os processos de forma a estabelecer métricas de performance sob as políticas, objectivos, requisitos e atividades planeadas. Reportar os resultados.

4. Act (Melhoria)

Desenvolver ações de forma a melhor a performance conforme necessário.



O Ciclo PDCA é um exemplo de um sistema de ciclo fechado. Este ciclo garante que cada lição aprendida na fase de Do e Check é canalizada para as fases Act e Plan, adicionando assim know-how a cada nova fase subsequente.

6

Pensamento baseado no Risco

A metodologia para implementação consiste nos seguintes passossequenciais, em alinhamento com o definido na norma ISO 10019:

Auditoria de Diagnóstico	1
Clarificação de requisitos	2
Auditoria de Diagnóstico	3
Definição do representante da gestão e interlocutor	4
Definição da estratégia e processos	5
Plano de ação	6
Identificação dos recursos necessários	7
Formação dos intervenientes	8
Desenvolvimento documental e implementação	9
Auditoria interna	10
Revisão do sistema	11
Consolidação e melhoria	12
Auditoria de Certificação	13

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

1. Auditoria de Diagnóstico

Será realizada uma auditoria de Gap-Analysis de forma a realizar um levantamento inicial sobre o estado da arte da organização relativamente aos requisitos da norma de Sistema de Gestão

2. Clarificação de requisitos

Informação à gestão de topo da sobre os requisitos principais da norma dos sistemas de gestão, e os papéis da organização para a conceção e desenvolvimento do Sistema de Gestão.

3. Análise de necessidades e expectativas

Análise das necessidades e expectativas das partes interessadas da Organização.

4. Definição do representante da gestão e interlocutor

Nomeação de um representante da gestão e estabelecimento de definições de política, objetivos e compromissos para com o referencial do Sistema de Gestão. Desenvolvimento dos objetivos a níveis funcionais apropriados na organização.

5. Definição da estratégia e processos

Após o levantamento inicial, são estabelecidos os diferentes processos. Para tanto, recorre-se:

- Análise detalhada da estrutura, processos, canais de comunicação e interfaces existentes na organização;
- Identificação dos processos e responsabilidades para atingir os objetivos;
- Definição da sequência de interações entre os processos tratados acima.

6. Plano de ação

O Plano de ações resultará da fase anterior, sendo suportado no conhecimento da realidade da organização e das condicionantes - requisitos legais, normativos e do cliente e Política da organização.

7. Identificação dos recursos necessários

Os Sistemas de Gestão conduzem a algumas mudanças nas organizações que não podem ser obtidas por decreto, resultando antes de uma atitude positiva, motivadora e dinâmica, devendo ser assumida com todas as suas implicações e consequências. Uma condição fundamental para que tal ocorra, será o envolvimento efetivo de todos os Recursos Humanos da Organização, e muito especialmente das Administrações e Direções, que se deverão assumir como elementos dinamizadores do processo e cuja exemplaridade na ação será imprescindível.

8. Formação dos intervenientes

Durante o desenvolvimento / implementação do Sistema deverão ser efetuadas ações de sensibilização junto das chefias e colaboradores, com o objetivo de as envolver e comprometer na implementação do mesmo.

9. Desenvolvimento documental e implementação

Para a sustentação do Sistema de Gestão, é igualmente fundamental definir a estrutura documental necessária para a normalização do sistema.

10. Auditoria interna

O objetivo desta fase será a avaliação, por uma Equipa Auditora independente, da conformidade do Sistema implementado.

11. Revisão do sistema

Após a fase de Auditoria interna, é necessário efetuar a revisão periódica do sistema de gestão, com o devido envolvimento da gestão de topo.

12. Consolidação e melhoria

Esta fase, consistirá fundamentalmente na implementação das Ações Corretivas, Preventivas e de Melhoria, decorrentes da Auditoria Interna, com o objetivo de testar e assegurar a funcionalidade e a eficácia do Sistema de Gestão

13. Auditoria de Certificação

será realizada uma auditoria por parte de uma entidade certificadora devidamente acreditada de forma a garantir a conformidade com o referencial do Sistema de Gestão. Após auditoria positiva, a organização estará certificada, entrando no respetivo ciclo de certificação.

7

Pensamento baseado no Risco

A Gestão Integrada de Sistemas de Gestão é implementada há cerca de 20 anos, conferindo às organizações uma abordagem eficaz de forma a atingirem os seus objectivos de uma forma eficiente.

As vantagens e benefícios dos sistemas de gestão integrados (SGI) são reconhecidos internacionalmente, levando ao desenvolvimento de metodologias, como a PAS 99:2006v do British Standards Institute (BSI) e, mais recentemente, em 2018, a publicação do IUMSS1 Handbook, do Comité Técnico ISO/TMB/JJCGTF 05, compilando vários exemplos de implementação em diversos setores de atividade, bem como boas práticas na implementação de sistemas de gestão integrados.

A principal lição a ser retirada do líder do grupo de trabalho da ISO é clara e conclusiva: "Muitas organizações utilizam múltiplos sistemas de gestão para garantir que os seus sistemas e processos estão alinhados com os seus objectivos e para manter o seu modelo de negócio num ambiente em constante mudança".

Como um sistema de gestão integrado pode ser adaptado de acordo com as necessidades da organização, não existe um único modelo disponível. De qualquer forma, o sistema de gestão integrado mais comum é o sistema de gestão da Qualidade, Ambiente e Segurança e, na generalidade das organizações, existem benefícios claros, tais como:

- Aumento de eficácia, eficiência e melhoria baseada na otimização dos processos e atividades da organização;
- Redução das repetições e lacunas que ocorrem quando os sistemas de gestão são geridos de forma individual;
- Melhoria no foco nos objectivos da organização e expectativas das partes interessadas;
- Aumento da confiança da gestão de topo na implementação e manutenção das políticas.

A abordagem integrada aos sistemas de gestão ajuda as organizações a um nível estratégico, levando assim a um maior foco nos objectivos a médio e longo prazo, invés da melhoria apenas a curto prazo.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

O desenvolvimento de um Sistema Integrado de Gestão deverá ser suportado por conceitos devidamente pensados e coerentes. Este Sistema tem associado:

- **CLIENTE**
  o cliente é neste conceito um cliente com "C" maiúsculo. O CLIENTE engloba:
  - O Consumidor - associado à vertente Qualidade. Neste campo, é esperado por parte deste CLIENTE conformidade do produto ou serviço para desempenhar as funções esperadas;
  - O Colaborador - Do desenvolvimento dos processos, espera da parte da organização, conformidade com os requisitos normativos e legais, associados à prevenção de riscos;
  - A Sociedade - associado ao Contexto Externo. Os processos associados à Organização são avaliados, verificando conformidades a nível externo, de modo que o impacte seja menos significativo possível.
- PRODUTO - o Produto e/ou serviço é o output contínuo dos processos, somatório do bem adquirível pelo consumidor, dos riscos para o trabalhador e do impacte ambiental para a sociedade.

A Gestão Integrada tem vindo a ser implementada em diversas organizações, com vantagens inequívocas, como sejam:

- Simplificação da estrutura orgânica, pela criação de um único órgão funcional;
- Simplificação de processos e procedimentos, representando um menor envolvimento de recursos para a manutenção e melhoria do Sistema, contribuindo, assim, para uma maior competitividade da Organização;
- Igualar ou obter vantagem competitiva sobre a concorrência e aumentar a motivação interna;
- Melhorar a imagem da organização, externa e interna;
- Concentração nos objetivos da organização e nas expetativas do CLIENTE;
- Obtenção e manutenção da Qualidade a fim de satisfazer as necessidades do CLIENTE;
- Melhoria da execução, da coordenação global;
- Confiança da parte da Direção de que a qualidade pretendida está a ser atingida e mantida;
- Demonstração ao CLIENTE das capacidades da organização.

8

Cláusulas normativas da ISO 20858

Generalidades

A ISO 20858 é uma norma de requisitos destinada a ajudar as organizações que optam por implementar voluntariamente os requisitos, estabelecer e demonstrar sua conformidade com as directrizes da IMO e do o Código ISPS, no que concerne à segurança e proteção da IP, por forma a poder ser verificada por uma organização externa.

A norma é composta por 6 secções abordando designadamente a Avaliação de Proteção da Instalação Portuária (APIP), o Plano de Proteção da Instalação Portuária (PPIP), e a documentação atinente à proteção da IP, bem como a sua classificação de segurança e a respectiva salvaguarda.

As próximas secções deste manual apresentam as cláusulas da ISO 20858.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

Desenvolvimento da Avaliação de Proteção da Instalação Portuária (APIP)

Visão Geral da Avaliação de Proteção

A IP que implementa esta Norma deve conduzir uma avaliação de proteção ou basear-se em avaliações de proteção existentes que sejam válidas, documentadas e atendam aos requisitos expressos na Norma.

A APIP é parte integrante e essencial do processo de elaboração e actualização do PPIP.

A avaliação deve considerar cenários de ameaças à segurança, consequências de um ataque bem sucedido à instalação portuária e a probabilidade de cada cenário de ameaça à segurança ser bem sucedido, considerando as medidas de segurança em vigor.

Devem, igualmente ser ponderadas medidas adicionais de proteção, se se considerarem necessárias.

A avaliação da protecção da instalação portuária será periodicamente revista e actualizada, tendo em conta a evolução das ameaças e/ou as modificações menores efectuadas na instalação portuária e deve ser revista e actualizada sempre que a instalação portuária sofra modificações importantes

Pessoal que conduz a APIP

Para um eficaz e eficiente desenvolvimento da APIP, é fundamental que os avaliadores tenham competência para aferir da protecção da instalação portuária, bem como um conhecimento detalhado das operações da IP, suas instalações, medidas de proteção em vigor, possíveis ameaças, inclusive em locais específicos.

O pessoal envolvido numa APIP poderá ter que contar com colaboradores externos especializados em múltiplos aspectos relativos a segurança e protecção Todo o pessoal envolvido numa APIP, incluindo os colaboradores externos referidos supra, deve ser listado no Relatório de Avaliação de Proteção da Instalação Portuária.

Âmbito do desenvolvimento da APIP

A APIP deverá englobar as instalações portuárias e infraestruturas portuárias que possam ser ameaçadas ou utilizadas para ameaçar o comércio marítimo, devendo incluir no mínimo, todas as áreas e equipamentos:

- Onde decorram as operações especificas da IP;
- Onde a carga é recepcionada, arrumada ou manuseada antes e depois do seu transporte por via marítima;

Onde a documentação relativa à carga e ao Onde a documentação relativa à carga e ao seu transporte marítimo é seu transporte marítimo é manuseada e arquivada;

- Anexas ao perímetro de segurança da IP;
- Incluindo os canais de navegação, praticados pelos navios na sua de aproximação à IP;

Estas áreas deverão ser objecto de uma análise exaustiva e criteriosa relativa aos requisitos de proteção, tendo por base uma lista de avaliação das medidas de proteção.

Apresenta-se abaixo um extracto da Lista de Avaliação das Medidas de Proteção – que serve de guião base ao desenvolvimento da APIP Pessoal que conduz a APIP.

Para um eficaz e eficiente desenvolvimento da APIP, é fundamental que os avaliadores tenham competência para aferir da protecção da instalação portuária, bem como um conhecimento detalhado das operações da IP, suas instalações, medidas de proteção em vigor, possíveis ameaças, inclusive em locais específicos.

O pessoal envolvido numa APIP poderá ter que contar com colaboradores externos especializados em múltiplos aspectos relativos a segurança e protecção.

Todo o pessoal envolvido numa APIP, incluindo os colaboradores externos referidos supra, deve ser listado no Relatório de Avaliação de Proteção da Instalação Portuária.

8 Cláusulas normativas da ISO 20858

Âmbito do desenvolvimento da APIP

A APIP deverá englobar as instalações portuárias e infraestruturas portuárias que possam ser ameaçadas ou utilizadas para ameaçar o comércio marítimo, devendo incluir no mínimo, todas as áreas e equipamentos:

- Onde decorram as operações especificas da IP;
- Onde a carga é recepcionada, arrumada ou manuseada antes e depois do seu transporte por via marítima;

Onde a documentação relativa à carga e ao seu Onde a documentação relativa à carga e ao seu transporte marítimo é seu transporte marítimo é manuseada e arquivada;

- Anexas ao perímetro de segurança da IP;
- Incluindo os canais de navegação, praticados pelos navios na sua de aproximação à IP;

Estas áreas deverão ser objecto de uma análise exaustiva e criteriosa relativa aos requisitos de proteção, tendo por base uma lista de avaliação das medidas de proteção.

Apresenta-se abaixo um extracto da Lista de Avaliação das Medidas de Proteção – que serve de guião base ao desenvolvimento da APIP

A IP dispõe documentos e procedimentos que comtemplem os aspectos seguintes?	**Sim**	**Não**	**Comentários**
1 Organização de segurança da IP			
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			

Deverão ser igualmente analisadas e avaliadas as condições atinentes à proteção, nos bens e activos da IP, em função dos danos ou perdas que poderiam sofrer se uma ameaça se materializasse contra eles, não apenas no interior da IP, mas também nas suas áreas adjacentes.

Toda esta avaliação deverá ser objecto de registo e documentação específica.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

8 Cláusulas normativas da ISO 20858

Contactos com Forças e Serviços de Segurança do Estado (FSSE)

Devem ser estabelecidos contactos com as FSSE apropriados, tendo em vista avaliar:

- Potenciais ameaças à IP;
- Aspectos particulares das IPs e dos navios que demandem a IP que possam ser alvo de um ataque;
- Consequências de perdas de vida, danos à propriedade, perturbações económicas, incluindo perturbações nos sistemas de transporte, de um ataque às IP;
- As capacidades e intenções de eventuais perpetradores de ataques à IP ou navios que a demandem;

A informação recebida deve ser devidamente registada e, no aplicável, ser tida em consideração.

Se as FSSE não desejarem participar no contacto ou reunião, a organização que desenvolve a APIP, deve documentar sua (s) tentativa (s) e declarar que as aquelas forças não participaram nesta iniciativa.

Os aspectos descritos supra configuram uma identificação de ameaças à IP e às suas áreas envolventes. Esta actividade é complexa e eivada de incerteza, uma vez que envolve a análise de múltiplas hipóteses de ameaças e da natureza diferenciada da sua possível materialização, motivações dos seus perpetradores, timing e oportunidade da sua ocorrência. Neste aspecto particular, a norma contempla a identificação de cenários de ameaça e a possibilidade de materialização dos mesmos.

Avaliação de consequências

Uma avaliação das consequências dos incidentes de proteção deve ser conduzida e, deve considerar potenciais perdas de vidas, perdas económicas, impacto ambiental, e outras relevantes.

As consequências de cada incidente de proteção avaliado numa IP serão classificadas como alto, médio ou baixo.

Classificação da Probabilidade da Ocorrência de Cenários de Proteção

O estado das medidas de proteção física e operacional, conforme documentado na lista de avaliação das medidas de proteção e, outros dados que se mostrem relevantes para avaliar as medidas de proteção, devem ser considerados para se proceder a uma classificação de possíveis cenários de proteção.

Medidas de proteção física incluem objectos que impeçam ou detectem o acesso não autorizado a um alvo.

As medidas de proteção operacional incluem pessoas e procedimentos que que impeçam ou detectem o acesso não autorizado a um alvo.

A probabilidade de cada cenário de proteção se tornar um incidente de proteção em relação a um determinado activo deve ser classificada como alta, média e baixa.

- A probabilidade alta deve ser usada quando as medidas de proteção em vigor oferecem pouca resistência a esse incidente de proteção.

- A probabilidade média deve ser usada quando as medidas de proteção em vigor oferecerem resistência moderada a esse incidente de proteção.

- A probabilidade baixa deve ser usada nos casos em que as medidas de proteção em vigor ofereçam resistência substancial a esse incidente de proteção

A justificação para a classificação da probabilidade atribuída a cada cenário de proteção deve ser devidamente fundamentada e documentada.

Este processo de avaliação, análise e classificação dos incidentes de proteção deverá permitir conduzir à determinação da necessidade da implementação de contramedidas.

8 Cláusulas normativas da ISO 20858

Assim, a definição de Contramedidas é função da Probabilidade e da Consequência da ocorrência de um dado cenário de proteção, que se apresenta na imagem seguinte:

Probabilidade	Consequência: Alta	Consequência: Média	Consequência: Baixa
Alta	contramedidas	contramedidas	
Média	contramedidas		
Baixa			

A identificação de contramedidas é necessária para os cenários de proteção classificados de alta e média probabilidade de ocorrência e de alta consequência, juntamente com os que são classificados como de alta probabilidade e média consequência.

Outros cenários de proteção não carecem, em princípio, de contramedidas, excepto se o(s) avaliador(es) considerarem que, de facto se justifique a sua implementação. O(s) avaliador(es) de proteção deve(m) listar e documentar cada cenário de proteção que determine a necessidade de implementação de contramedidas.

Contramedidas

Cada contramedida deve ser avaliada quanto à eficácia em reduzir a probabilidade de ocorrência ou as respectivas consequências (ou uma combinação de ambas) até que o cenário de proteção não exija que as contramedidas sejam consideradas.

Cada contramedida que cumpra estes requisitos, deverá ser listada no PPIP.

Plano de Proteção da Instalação Portuária (PPIP)

Visão geral do PPIP

De acordo com o estabelecido na parte B, 16 código ISPS o PPIP é basicamente um documento classificado, redigido na língua de trabalho da instalação portuária, repositório completo e rigoroso da descrição do funcionamento da segurança da IP visando proteger o pessoal, a infraestrutura, navios atracados, carga, unidades de transporte de carga (contentores) e sobressalentes dos navios que demandam a IP, dos riscos de um incidente de proteção.

O PPIP terá por base os cenários identificados na APIP, a identificação de meios, medidas, procedimentos e contramedidas que visam diminuir o grau de risco identificado para cada cenário considerado na APIP.

O PPIP especifica responsabilidades da administração da IP e do Oficial de Proteção da IP, constituindo um importante elemento para possibilitar a formação dos colaboradores, em particular dos que estão afectos à segurança e proteção da IP, permitindo igualmente o desenvolvimento de treinos e exercícios, que se revelam importantes para criar automatismos relevantes, permitindo verificar a adequabilidade dos procedimentos, e constatar, se na prática, há procedimentos que se mostram desadequados ou menos adequados à realidade das operações e funcionamento da IP.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

8 Cláusulas normativas da ISO 20858

Âmbito do desenvolvimento do PPIP

O PPIP deverá abranger os perímetros e áreas que foram considerados na APIP (descritos no ponto 8.2.3 deste manual), bem como designadamente:

- Todas as portas e pontos de acesso (funcionais ou não);
- Áreas restritas nas IPs;
- Cais e / ou pontões de atracação de navios e embarcações;
- Equipamentos de emergência e controlos de paragem 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 (a menos que a carga esteja misturada com materiais não perigosos – aspecto que deve ser anotado);
- Infraestruturas críticas dentro da IP. tica, há procedimentos que se mostram desadequados ou menos adequados à realidade das operações e funcionamento da IP.

8 Cláusulas normativas da ISO 20858

Estrutura Funcional de Proteção da IP

A Proteção afeta todas as áreas da IP, pelo que é necessário assegurar a sensibilização e capacitação de todos os colaboradores da mesma.

A gestão de topo da IP tem a responsabilidade de estabelecer e capacitar uma estrutura organizacional de proteção da IP.

O PPIP especifica obrigatoriamente:

- Uma descrição da estrutura organizacional de proteção, incluindo uma explicação dos deveres e responsabilidades de cada pessoa no âmbito da mesma.
- Uma descrição de responsabilidades e funções, englobando designadamente:
  - A gestão da proteção;
  - Oficial de Proteção da IP (OPIP) – devendo ser, igualmente, especificada a sua identificação e a forma de ser contactado a qualquer momento (H24). O código ISPS refere sucintamente as funções e responsabilidades do 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.

Alterações nos níveis de proteção

O PPIP deve definir procedimentos para:

- Garantir que a instalação opere em conformidade com o nível de segurança exigido em vigor na IP.
- Garantir que todos os requisitos adicionais de segurança estão em vigor, incluindo a notificação de navios a cais, a entrar ou a largar da IP, quando houver um aumento no nível de segurança.
- Nos Níveis de Segurança 2 e 3, assegurar que o OPIP esclareça todos os colaboradores da IP sobre as ameaças de segurança identificadas, enfatizando os procedimentos de reporte de incidentes e a necessidade de reforçar a vigilância.

Procedimentos de interface com os navios

O PPIP especifica medidas para interface com navios em todos os níveis de segurança.

Declaração de Proteção (DoS – Declaration of Security)

Relativamente à DoS o PPIP define procedimentos:

- Para a solicitar;
- Para tramitar as solicitações do(s) navio(s);

Requisitos adicionais para instalações portuárias que recebem navios de passageiros no Nível de Proteção 1

O PPIP deve descrever os procedimentos tomados antes da chegada de um navio às IPs, em que o OPIP, o Comandante e o Oficial de Segurança do Navio (OSN) (ou seus representantes, devidamente identificados) coordenam as necessidades e procedimentos de segurança enquanto o navio estiver na IP.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

8 Cláusulas normativas da ISO 20858

Comunicações

O PPIP deve referir expressamente os meios pelos quais o OPIP pode notificar o pessoal da instalação sobre mudanças nas condições de segurança, assente num sistema de comunicações ágil e eficaz.

Este sistema deve permitir comunicações contínuas e fiáveis entre:

- O pessoal de segurança das IP;
- Os navios que fazem interface com a instalação;
- O OPIP e as Forças de Segurança nacionais e / ou locais.

Em cada ponto de acesso e / ou portaria de acesso à IP, deve estar disponível um sistema de comunicações para que o pessoal que exerce funções de vigilância e segurança nesses pontos possa contactar:

- As Forças de Segurança;
- O controlo de segurança ou um Centro de Operações de Emergência via telefone fixo, telefone móvel ou rádios portáteis;

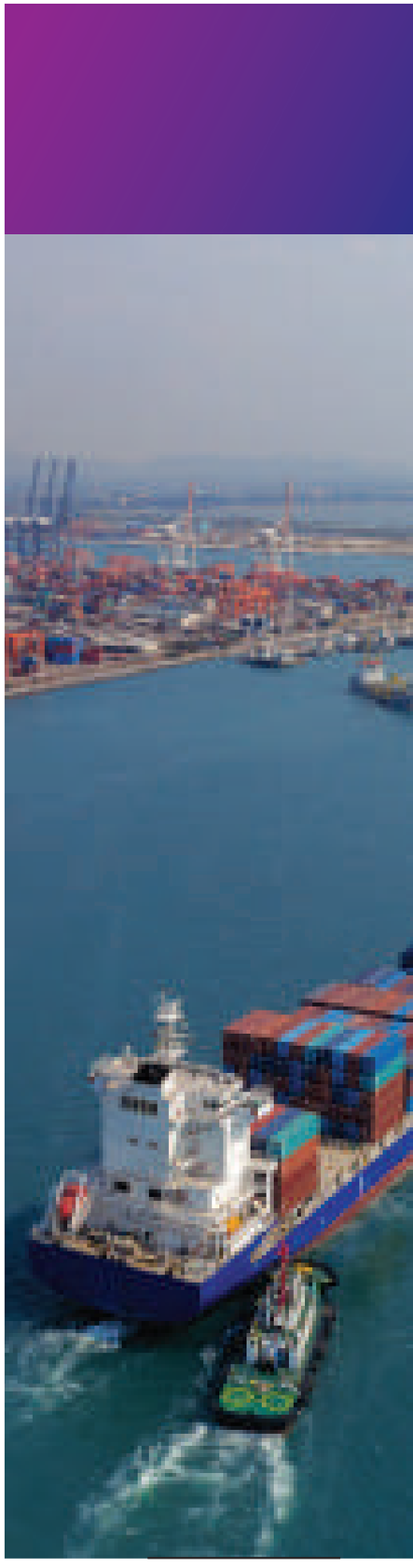
O sistema de comunicações da IP deve ter redundância para permitir que quer as comunicações de segurança e proteção internas e externas internas e / ou externas se estabelecem de forma rápida e eficaz, para que as necessárias medidas possam ser implementadas com rapidez e eficiência.

Manutenção dos Equipamentos de Proteção

Os procedimentos neste âmbito devem estar clarificados no PPIP, por forma a que sejam contemplados os seguintes requisitos:

- Os sistemas e equipamentos de segurança devem estar em boas condições de funcionamento, devendo ser inspecionados, testados, calibrados e mantidos de acordo com as recomendações dos fabricantes;
- As deficiências do sistema de segurança devem ser corrigidas prontamente e os resultados registrados.
- Devem ser incluídos procedimentos para identificar e responder a falhas ou deficiências de funcionamento do sistema de segurança e respectivos equipamentos.

O sistema de comunicações da IP deve ter redundância para permitir que quer as comunicações de segurança e proteção internas e externas



8 Cláusulas normativas da ISO 20858

Medidas de proteção para controle de acesso, incluindo áreas de acesso público

Aspectos gerais

O PPIP deverá definir medidas de proteção por forma a:

- Proteger a IP da introdução de substâncias perigosas e dispositivos perigosos, incluindo qualquer dispositivo destinado a danificar ou destruir pessoas, ou navios;
- Efectuar um rigoroso controlo de acessos de pessoas e bens à IP, incluindo a emissão de cartões de acesso de pessoas autorizadas;
- Efectuar a verificação de bagens, mercadorias, bens e fornecimentos que entrem na IP, utilizando para o efeito, se necessário, dispositivos de detecção de metais, equipamentos de raios X, ou outros que sejam utilizáveis por pessoal adstrito à segurança da IP;
- Outras medidas que visem monitorizar o controlo de acesso de pessoas, bens e fornecimentos à IP ou aos navios que estejam no seu interior.

Aspectos particulares

O PPIP definirá expressamente medidas de segurança adicionais deste âmbito, para os níveis de proteção 2 e 3.

Medidas de proteção para áreas restritas

O PPIP deve definir as áreas restritas nas instalações portuárias, especificando todas as que se constituem como infraestruturas críticas para operação, proteção e continuidade do negócio da IP (para além das já referidas no ponto 8.3.2, e em especial as áreas que enquadram: informações confidenciais de segurança; documentação de carga; equipamentos e sistemas de segurança, e de vigilância e, respectivos controlos; sistemas de abastecimento de água, de telecomunicações e sistemas elétricos; áreas de carga e armazenamento de carga composta por mercadorias perigosas).

Acesso a áreas restritas

Serão obrigatoriamente definidos os procedimentos para:

- Determinar quais as pessoas, para além do pessoal da IP, que estão autorizadas a ter acesso às áreas restritas, definindo expressamente as condições em que esse acesso deve ocorrer;
- Controlo e registo de todos os movimentos de pessoas, cargas, descargas e / ou quaisquer outras manobras ou operações nas áreas restritas;
- Estabelecer medidas de coordenação com os transportadores, fornecedores e prestadores de serviço que tenham que ter acesso às áreas restritas, por forma a identificar e controlar eficazmente o movimento do respectivo pessoal, e bem assim como cargas e / ou bens que transportem para e / ou da IP, incluindo o rigoroso controlo de movimento, carga e descarga de mercadorias ou substâncias perigosas, utilizando para o efeito todos os dispositivos que se mostrem adequados para a inspeção destas sustâncias, e com a regularidade que for entendida como necessária.
- O PPIP definirá ainda claramente medidas de segurança adicionais deste âmbito, para os níveis de proteção 2 e 3.

Medidas de proteção para entrega de carga destinada a armazéns de apoio aos navios na IP

Estarão especificados no PPIP os procedimentos de segurança e proteção relativos à entrega de componentes e carga destinados a apoiar logisticamente os navios que demandem IP, assegurando que, se necessário todos os itens são verificados e controlados, bem como registados os transportadores e respectivo pessoal que fez chegar os referidos itens aos armazéns de apoio aos navios.

O PPIP definirá expressamente medidas de segurança adicionais deste âmbito, para os níveis de proteção 2 e 3.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

8 Cláusulas normativas da ISO 20858

Medidas de proteção de vigilância da IP

- Toda as áreas da IP, e com particular enfoque nas áreas restritas, quer do lado de terra quer do lado dos acessos da frente marítima têm que estar sujeitas a delimitação, vigilância e monitorização continuas, por meio de uma combinação de iluminação, sistemas de vídeo vigilância (CCTV), pessoal adstrito à segurança, detetores automáticos de intrusão, e / ou outros que a especificidade da IP assim o exigir.

O PPIP definirá medidas adicionais de proteção e vigilância a serem adoptadas nos níveis de proteção 2 e 3.

Procedimentos em incidentes de segurança / proteção

O PPIP descreverá os procedimentos que garantam que o pessoal de segurança da IP estará apto a:

- Responder a ameaças de segurança ou violações de segurança, por forma a garantir que as instalações críticas da IP, possam continuar em funcionamento;
- Evacuar a instalação em caso de ameaças de segurança ou violações de segurança;
- Relatar eficazmente os incidentes de segurança;
- Informar todos os colaboradores da IP sobre possíveis ameaças à segurança, necessidade de vigilância, solicitando o relato e identificação de pessoas, objetos ou atividades suspeitas;
- Proteger operações não críticas para focar respostas em operações críticas da IP.

Requisitos adicionais para instalações de passageiros e ferry boats

Se a IP receber navios de passageiros ou ferries, o PPIP deverá detalhar:

- Medidas de proteção para controlo e vigilância de passageiros e / ou de veículos que embarquem e desembarquem dos ferry boats;
- Estabelecer áreas de acesso público, devidamente controladas e vigiadas por pessoal adstrito à segurança da IP em número e qualidade suficientes para, se necessário monitorizar e inspecionar passageiros, suas bagagens, e pertences, e bem assim como verificação e controlo dos veículos, seu interior e carga;
- Definir áreas especificas para proceder a identificação, revistas e inspeção dos passageiros, suas bagagens, e pertences, e bem assim como possibilitar as mesmas ações aos veículos, seu interior e carga. Estas operações de segurança e proteção devem ser adequadas ao nível de proteção que estiver em vigor na IP;
- Negar o acesso de passageiros a áreas restritas, a menos que o pessoal de segurança da IP possa controlar eficazmente os respectivos acessos a essas áreas.

O PPIP definirá claramente medidas de segurança adicionais deste âmbito, para os níveis de proteção 2 e 3.

8 Cláusulas normativas da ISO 20858

Requisitos adicionais em terminais de cruzeiros

No caso de terminais de passageiros de navios de cruzeiros o PPIP deverá clarificar as medidas de segurança e proteção, por forma a permitir:

- Rastear todas os passageiros, bagagens e objetos pessoais, designadamente possibilitando a detecção de substâncias e / ou dispositivos perigosos;
- Verificar a identificação de todas as pessoas que desejam embarcar no navio, incluindo a confirmação da razão do seu embarque, examinando instruções de acesso, bilhetes de viagem, cartões de embarque, identificação pessoal através de documentos emitidos pelas autoridades do país de nacionalidade respectivo;
- Dotar a IP de áreas de espera e de embarque separadas que permitam concentrar os passageiros, suas bagagens e pertences pessoais a controlar, separando os passageiros, suas bagens e pertences que já tenham sido verificados, e controlados enquanto aguardam o respectivo embarque;
- Dispor de pessoal de segurança adicional para controlo e vigilância nas das áreas designadas de espera e / ou de embarque;
- Negar o acesso de passageiros a áreas restritas, a menos que o pessoal de segurança da IP possa controlar eficazmente os respectivos acessos a essas áreas.

Auditorias e alterações ao PPIP

O PPIP deverá definir claramente a política da IP tendente à revisão periódica do Plano de Proteção da Instalação Portuária, e a forma de ser auditado e revisto conforme necessário, e sempre que haja alterações nas infraestruturas e operações da IP.

Competências, do pessoal de segurança das IP

O PPIP deve clarificar o programa de treino e adestramento do pessoal de segurança da IP, estabelecerá claramente as respectivas competências e capacidades, designadamente as que estão expressas no código ISPS (partes B 18.1 a B 18.3), bem assim como definirá os sistemas de avaliação necessários para aferir as consequentes competências e capacidades no decurso de ações de treino, adestramento e exercícios.

Treinos e exercícios

O PPIP define a política e os procedimentos para que o OPIP realize

pelo menos uma acção de treino do pessoal de segurança da IP a cada 3 e, um grande exercício por ano que englobe toda a IP e seus colaboradores. O período entre os treinos e os exercícios especificados não poderá ser superior a 18 meses.

Os treinos e exercícios devem testar os vários aspectos do PPIP, e devem incluir situações e cenários que incluam as respostas a ameaças e incidentes de proteção, como por exemplo:

- Entrada(s) não autorizada em área(s) restrita(s);
- Resposta a alarmes e avisos às autoridades policiais.

Se um navio estiver atracado na instalação na data em que se planeou realizar qualquer treino ou exercício, a Administração da IP poderá convidar, mas não poderá exigir, que o navio participe da simulação programada da instalação.

Manual de Boas Práticas desenvolvido com base na norma ISO 20858:2007

8 Cláusulas normativas da ISO 20858

Execução do plano de segurança da cadeia de abastecimento

Como se refere no ponto 2 deste manual a implementação de um Sistema de Gestão de Segurança da IP e a sua certificação segundo a ISO 20858, tendo por base o PPIP, permite estabelecer um sistema de gestão que possibilita que os processos específicos de segurança e proteção sejam implementados, por forma a alcançar o desiderato da segurança e proteção da operação da IP e do adequado funcionamento da cadeia de abastecimento em que ela se insere.

Documentação

A APIP, o PPIP e toda a documentação de suporte necessária ao desenvolvimento daqueles documentos, bem como todos registos e relatórios relacionados com a segurança e proteção da IP (ações de treino, adestramento, exercícios, incidentes de proteção, alterações de níveis de segurança, registos relativos aos equipamentos de proteção, suas condições de operação, registos de manutenção e ocorrências, entre outros) devem ser arquivados e salvaguardados para evitar divulgações não autorizadas, os procedimentos para permitir aquele objectivo devem ser claramente definidos no PPIP.

9

Certificação

A certificação é o processo no qual, através do recurso a uma entidade externa e independente à organização, devidamente acreditada para esse efeito – o organismo de certificação ou entidade certificadora – é emitido um certificado que atesta que determinado produto, processo ou serviço está em conformidade com os requisitos de um dado referencial.

O processo de certificação é um processo voluntário, podendo recorrer a este serviço qualquer entidade, independentemente do seu estatuto ou domínio de atividade.

O processo de certificação tem por base a Auditoria de Certificação. As auditorias de concessão são realizadas em 2 fases distintas. Na 1ª fase da auditoria, a equipa auditora tem a oportunidade de ter um primeiro contacto com a organização auditada e efetuar uma avaliação prévia da sua estrutura organizacional e dos seus processos, tendo como objetivo final a identificação dos aspetos significativos que poderão ser consideradas não-conformes durante a 2º fase da auditoria de concessão.

Para a organização auditada, esta metodologia de avaliação tem a vantagem de lhe permitir, caso seja considerado como adequado, rever, corrigir e melhorar o seu sistema de gestão implementado de modo a reunir as condições essenciais para o sucesso da avaliação da conformidade durante a 2ª fase da auditoria.

As constatações levantadas na 2ª fase da auditoria deverão ser tratadas através de ações corretivas, sendo que é necessário a demonstração de evidências de implementação à entidade certificadora. Aposto a aprovação dessas ações, a entidade certificadora emite o Certificado.

Os ciclos de certificação são compostos por 3 anos:

- Auditoria de Concessão (1ºano) ou Renovação (ciclos seguintes);
- Auditorias de Acompanhamento (2º e 3º ano).

Referências

1. ISO 20858 - *Ships and marine technology - Maritime port facility security assessments and security plan development*
2. Regulamento (CE) nº 725/2004 do Parlamento Europeu e do Conselho de 31 de Março de 2004 - Jornal Oficial da União Europeia, 29/4/2004
3. ISO 31000 - *Risk Management - Principles and Guidelines;*
4. ISO Guide 73, *Risk management - Vocabulary.*