QUALIseg
ENGENEERING AND MANAGEMENT

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

Sistema de Gestão da Segurança da Cadeia de Abastecimento (SGSCA)

Projecto:

GISAMP

Cofinanciado por:

REPÚBLICA PORTUGUESA
MAR

fundoazul

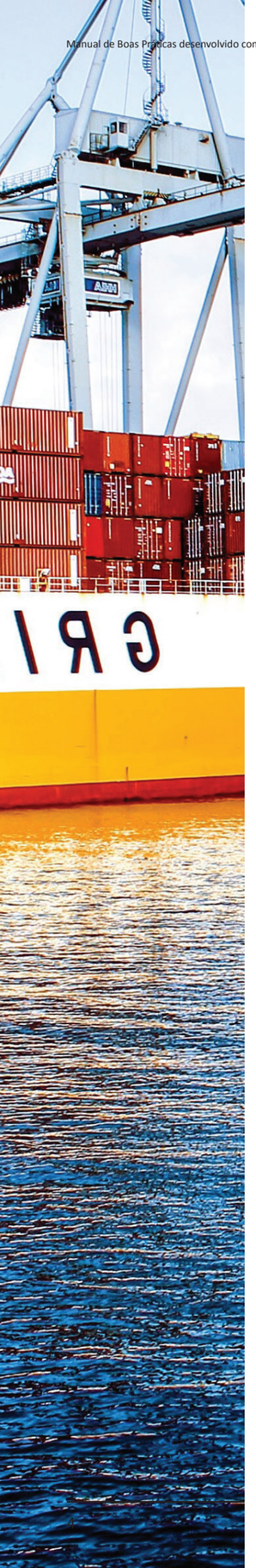
Índice

1. Introdução à norma ISO 28000 4
Enquadramento 4
A Família 28000 7
2. Benefícios da implementação da norma ISO 28000 8
3. Principais conceitos e terminologia 9
4. Pensamento baseado no Risco 10
5. Ciclo PDCA 13
6. Metodologia de implementação 14
7. Gestão Integrada 18
Anexo SL 19
8. Cláusulas normativas da ISO 28000 - Sistema de Gestão da Segurança da Cadeia de Abastecimento (SGSCA) 20
Requisitos gerais 21
Âmbito 21
Política de gestão da segurança 21
Apreciação e planeamento do risco de segurança 22
- Apreciação do risco de segurança 22
- Requisitos legais, estatutários e outros requisitos regulamentares de segurança 24
- Objetivos de gestão da segurança 24
- Metas de gestão da segurança 24
- Programas de gestão da segurança 24

Implementação e operacionalização 25
- Estrutura, autoridade e responsabilidades para a gestão da segurança 25
- Competência, formação e consciencialização 25
- Comunicação 26
- Documentação 26
- Controlo de documentos e dados 26
- Controlo operacional 26
- Preparação da emergência, resposta e recuperação da segurança 27

Verificação e ação corretiva 28
- Monitorização e medição do desempenho da segurança 28
- Avaliação do sistema 28
- Falhas, incidentes, não conformidades e ação corretiva e preventiva relacionados com a segurança 28
- Controlo dos registos 29
- Auditoria 29

Revisão pela gestão e melhoria contínua 30
9. Certificação 31
10. Referências 32
11. Anexos 33



1 Introdução à norma ISO 28000

Enquadramento

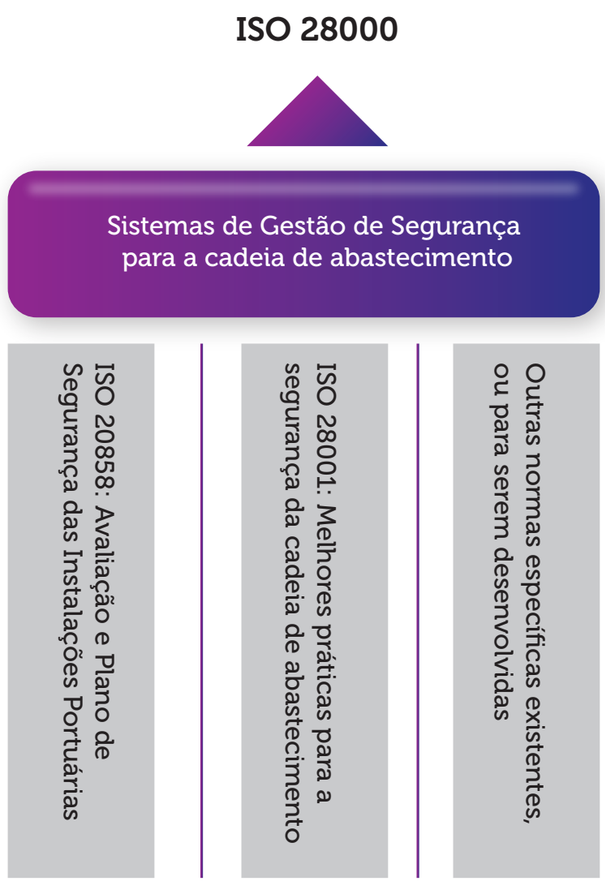
Quase todas as organizações dependem, de algum modo, de cadeias de abastecimento para garantir a continuidade dos negócios, tendo consciência que se tornam vulneráveis se essas cadeias forem interrompidas.

Consciente da importância de normalizar esta vertente, a ISO (Organização Internacional de Normalização) desenvolveu a norma ISO 28000 de gestão de segurança da cadeia de abastecimento, a qual fornece um modelo valioso para a identificação de riscos de segurança, para a implementação de controlos e de objetivos, visando a melhoria contínua da gestão de segurança e, por fim, facilitar a rápida circulação de bens na cadeia de abastecimento.

- A ISO 28000 é uma especificação de sistema de gestão que fornece, pela primeira vez, um modelo para todos os tipos e tamanhos de organizações que operam ou dependem de qualquer aspeto da cadeia de abastecimento. Compatível com várias normas de gestão, com particular relevo para a ISO 9001 e para a ISO 27001, a ISO 28000 foi desenvolvida com a finalidade de contribuir para a integração de sistemas de gestão, envolvendo, assim, a segurança da cadeia de abastecimento.
- Importa relevar que a ISO 28000 é compatível com iniciativas de segurança da Agência Alfandegária Internacional e Governos, assim como com outras ações complementares, tais como:
- Modelo de Normas da *World Customs Organization* para a segurança e facilitação da cadeia de fornecimento (WCO)
- Regulamento CE para a Melhoria da Segurança da Cadeia de Fornecimento – Operador Económico Autorizado (OEA)
- Alfândega dos EUA e Iniciativa de Proteção de Fronteiras (*Border Protection Initiative*) – Parceria Alfândega-Comércio contra o Terrorismo (*Customs Trade Partnership against Terrorism – C-PAT*).

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

A ISO 28000 – Sistema de Gestão de Segurança para a Cadeia de Abastecimento, sendo sustentada em diversos referenciais normativos (com destaque para: *ISO 28001 – Melhores Práticas para a Cadeia de Abastecimento* e *ISO 20858 – Avaliação e Plano de Segurança das Instalações Portuárias)*, permite a gestão integrada do risco de toda a cadeia de Abastecimento pelo seu nível de integração com outras normas, nomeadamente a *ISO 31000 – Gestão do Risco, ISO 14001 – Sistema de Gestão Ambiental, OHSAS 18001 – Sistema de Segurança e Saúde, ISO 27001 – Sistema de Gestão da Segurança da Informação e ISO 9001 – Sistema de Gestão da Qualidade.*



Assegurando todos os aspetos críticos que garantem a segurança da cadeia logística, a ISO 28000 trata dos aspetos organizacionais, legais, implementação das melhores práticas, metodologias e ferramentas, a segurança física, a segurança da informação, a inspeção das mercadorias, gestão dos sistemas de informação e gestão de incidentes.

1 Introdução à norma ISO 28000

A implementação da norma ISO 28000 a nível global está a conhecer uma evolução muito relevante, como é possível observar na tabela abaixo.

Entidades certificadas na ISO 28000

YEAR	2016	2017
Africa	1	5
Central / South America	53	59
North America	1	10
Europe	189	271
East Asia and Pacific	68	101
Central and South Asia	9	8
Middle East	35	40
TOTAL	**356**	**494**

Embora os dados da ISO ainda não estejam validados para 2018, estima-se que as entidades certificadas no final de 2018 ronde as 700.

Importa sublinhar que a norma ISO 28000 contribui para os United Nations Sustainable Development Goals, concretamente os objetivos 8, 9 e 11.

SUSTAINABLE DEVELOPMENT GOALS

1 Introdução à norma ISO 28000

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

A Família 28000

A série de normas 28000 engloba um conjunto de normas relevantes, com particular destaque para as seguintes:

- ISO 28001 – define as melhores práticas para a implementação das avaliações e planos da segurança na cadeia de abastecimento. Esta norma está concebida em linha com as normas e requisitos para facilitar o comércio global adotados pela World Customs Organization (WCO), pelo EU Customs Security Program-Authorized Economic Operator (AEO) e pela USA initiative – Customs Trade Partnership against Terrorism (CTPAT);

- ISO 28002 – estabelece requisitos para o desenvolvimento da resiliência na cadeia de abastecimento, assegurando que a cadeia de abastecimento de forma abrangente planeou adequadamente as ações adequadas para fazer face aos perigos e ameaças a que a cadeia está exposta;

- ISO 28003 – estabelece os requisitos para as entidades que devem auditar e/ou certificar o sistema de gestão de segurança da cadeia logística, definindo os requisitos para os auditores e os organismos de certificação, bem como uma série de requisitos para a realização das auditorias. Fornece aos clientes a informação necessária para que possam assegurar efetiva preparação para a auditoria de certificação;

- ISO 28004 – estabelece recomendações gerais para a implementação da ISO 28000, não contendo requisitos adicionais à ISO 28000. As suas diretivas ou indicações não são obrigatórias, indicando o que se "deveria" fazer (should), baseadas nas melhores práticas, podendo-se dizer que é nesta norma que está o conhecimento.

- ISO 28005 – define os requisitos para a transmissão eletrónica de dados Electronic port clearance (EPC) entre os elementos da cadeia de abastecimento, com potencial aplicação aos conceitos de Janela Única Portuária (JUP) e Janela Única Logística (JUL). O seu desenvolvimento foi efetuado em alinhamento com o Maritime Security Working Group.

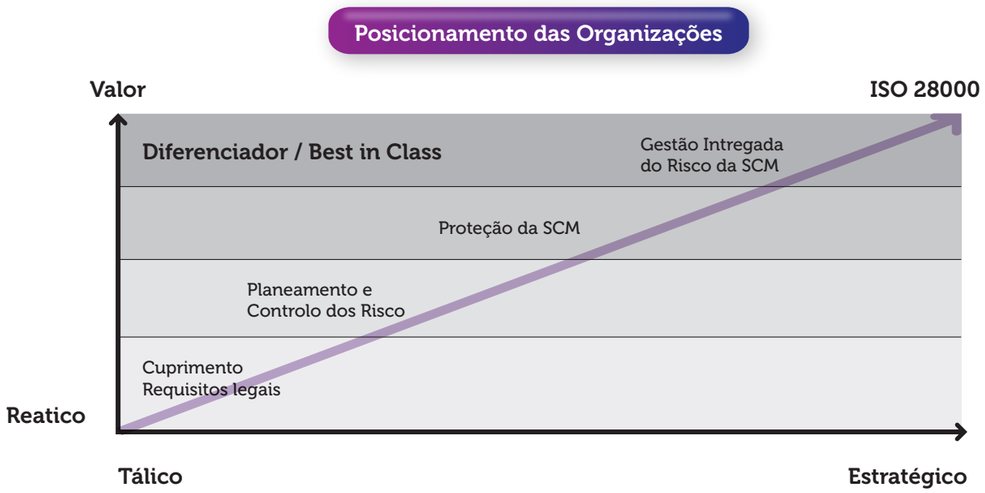
2

Benefícios da implementação da norma ISO 28000

A implementação da norma ISO 28000 permite às organizações um conjunto de benefícios relevantes, dos quais se destacam:

- Garante a execução de operações para a gestão de riscos e a implantação de medidas que o mitiguem, permitindo integração com outras normas de sistemas de gestão
- Enquadra para a definição de objetivos de segurança abrangentes, permitindo a melhoria contínua;
- Otimiza processos e possibilita consistência na execução em vários aspetos, demonstrando o cumprimento legal e interação com entidades reguladoras;
- Assegura o cumprimento dos requisitos exigidos pelas principais iniciativas internacionais (AEO, CTPAT, USCG...)
- Permite comunicar a clientes, autoridades, acionistas e investidores a implantação do sistema de gestão de segurança e utilizá-lo como ferramenta competitiva e diferencial
- Incentiva a colaboração e cooperação/interação entre várias entidades viabilizando soluções adequadas para problemas no fornecimento e entrega de produtos
- Define claramente as responsabilidades em todos os níveis da organização e fornece estrutura para rever sistematicamente os programas de segurança e para acompanhar e iniciar a melhoria contínua;
- Certificação de terceira parte do sistema de gestão de segurança da cadeia logística de uma organização em conformidade com padrões internacionais estabelecidos na norma ISO 28000.

É importante observar que a norma ISO 28000 pode ajudar significativamente as organizações a reforçar o seu Posicionamento Estratégico e a assumirem-se ao nível dos Best in Class nos seus setores. A imagem abaixo é ilustrativa dessa evolução.



Manual de Boas Práticas desenvolvido com base na norma ISO 28000

3

Principais conceitos e terminologia

Terminologia

A terminologia empregue ao longo do presente manual segue o disposto nas Normas Internacionais, com particular incidência na ISO 28000 e outras, concretamente a ISO 22300 e o guia ISO IEG Guide 73. Seguidamente apresenta-se a definição para os termos mais relevantes e/ou comumente empregues.

Instalação

Fábrica, máquinas, bens, edifícios, veículos, navios, instalações portuárias e outros elementos da infraestrutura ou da fábrica e sistemas relacionados que tenham uma função ou serviço de negócio distinto e quantificável.

NOTA: Esta definição inclui qualquer código de software que seja crítico para a entrega da segurança e para a aplicação da gestão da segurança.

Segurança

Resistência a ato(s) intencional(ais), não autorizado(s), destinado(s) a causar prejuízo ou dano a, ou através, da cadeia de abastecimento

Gestão da segurança

Atividades e práticas sistemáticas e coordenadas através das quais uma organização gere de forma otimizada os seus riscos, e os associados impactos e ameaças potenciais daí decorrentes

Objetivo da gestão da segurança

Resultado específico ou realização exigida pela segurança necessário à implementação da política de gestão da segurança

NOTA: É essencial que tais resultados estejam ligados de forma direta ou indireta ao fornecimento dos produtos, aos abastecimentos ou aos serviços oferecidos pela totalidade do negócio (ou da organização) aos seus clientes ou utilizadores finais.

Política de gestão da segurança

Conjunto de intenções e orientações de uma organização, relacionados com a estrutura e a segurança, para o controlo de processos e atividades relacionados com a segurança, que resultam e são consistentes com a política da organização e os requisitos regulamentares.

Programas de gestão da segurança

Meios através dos quais é alcançado um objetivo da gestão da segurança.

Meta da gestão da segurança

Nível específico de desempenho requerido para alcançar um objetivo da gestão da segurança

Segurança nas Sociedades

Proteção e resposta da sociedade a incidentes, emergências e desastres causados por atos humanos intencionais ou não intencionais, riscos naturais e falhas técnicas.

3 Principais conceitos e terminologia

Parte interessada

Pessoa ou entidade com interesse direto no desempenho e sucesso da organização ou no impacto das suas atividades.

NOTA: Exemplos incluem os clientes, os acionistas, os investidores, as seguradoras, as entidades reguladoras, os órgãos estatutários, os colaboradores, as entidades contratantes (ou subcontratados?), os fornecedores, as organizações sindicais ou a sociedade.

Cadeia de abastecimento

Conjunto de recursos e processos que começa com o fornecimento da matéria-prima e termina com a entrega dos produtos ou dos serviços ao utilizador final, incluindo os diversos modos de transporte.

NOTA *A cadeia de abastecimento poderá incluir os vendedores, os fabricantes, as transportadoras, os centros de distribuição interna, os distribuidores, os grossistas e outras entidades que conduzam ao utilizador final.*

A jusante

Refere-se às ações, processos e movimentos da mercadoria através da cadeia de abastecimento que ocorrem após a saída da mercadoria do controlo operacional direto da organização, que incluem mas não se limita ao seguro, a parte financeira, a gestão de dados, e o embalamento, o armazenamento e a transferência da mercadoria.

A montante

Refere-se às ações, processos e movimentações da mercadoria através da cadeia de abastecimento que ocorrem antes da saída da mercadoria do controlo operacional direto da organização, que incluem mas não se limita ao seguro, a parte financeira, a gestão de dados, e ao embalamento, o armazenamento e a transferência da mercadoria

Risco

Efeito da incerteza na consecução dos objetivos.

Gestão do risco

Atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco.

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.

Evento

Ocorrência ou alteração de um conjunto particular de circunstâncias.

Consequência

Resultado de um evento que afeta os objetivos.

Continuidade do negócio

Capacidade da organização para continuar a fornecer produtos ou serviços em níveis aceitáveis pré-definidos na sequência de um incidente disruptivo.

Desastre

Situação onde tenham ocorrido perdas humanas, materiais, económicas ou ambientais generalizadas que ultrapassam a capacidade da organização, comunidade ou sociedade afetadas para responder e recuperar usando os seus próprios recursos.

Crise

Situação com elevado nível de incerteza que interrompe as atividades essenciais e/ou a credibilidade de uma organização e que exige ação urgente.

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

3 Principais conceitos e terminologia

Perigo

Fonte de dano potencial.

Incidente

Situação que poderá ser ou conduzir a uma disrupção, perda, emergência ou crise.

Mitigação

Medidas tomadas para prevenir, limitar e reduzir o impacto das consequências negativas de incidentes, emergências e desastres.

Resiliência

Capacidade de adaptação de uma organização num ambiente complexo e em mudança.

Gestão de emergências

Abordagem global para a prevenção de emergências e gestão daquelas que ocorrem.

Gestão de topo

Pessoa ou grupo de pessoas que dirige e controla uma organização ao mais alto nível.

Sistema de gestão

Conjunto de elementos interrelacionados ou interatuantes de uma organização utilizados para estabelecer políticas, objetivos e processos para atingir esses objetivos.

Análise do impacto no negócio

Processo de análise das atividades e dos efeitos que uma disrupção no negócio poderá ter sobre elas.

Informação sensível

Informação que deve ser protegida de divulgação pública apenas porque teria efeito adverso numa organização, na segurança nacional ou na segurança pública.

Fonte de risco

Elemento que, por si só ou em combinação com outros, tem o potencial intrínseco de originar um risco.

Organização

Pessoa ou grupo de pessoas que tem as suas próprias funções com responsabilidades, autoridades e relacionamentos para atingir os seus objetivos.

Desempenho

Resultado mensurável.

Parceria

Relação organizada entre duas entidades (pública-pública, privada-pública, privada-privada) que estabelece o âmbito, os papéis, procedimentos e ferramentas para prevenir e gerir qualquer incidente com impacto na segurança nas sociedades no que respeita à legislação aplicável.

Acordo de apoio mútuo

Entendimento pré-estabelecido entre duas ou mais entidades para prestarem apoio entre si.

Programa de exercícios

Séries de eventos de exercício concebidos para se atingir um objetivo ou resultado global.

Capacidade

Combinação dos pontos fortes e recursos disponíveis numa organização, comunidade ou sociedade que podem reduzir o nível do risco ou os efeitos de uma crise.

Competência

Capacidade demonstrada para aplicar conhecimentos e técnicas para se atingir os resultados pretendidos.

Não conformidade

Não satisfação de um requisito.

Correção

Ação para eliminar uma não conformidade detetada.

Ação corretiva

Ação para eliminar a causa de uma não conformidade e para prevenir recorrência.

Risco residual

Risco que subsiste após tratamento do risco.

Conformidade

Satisfação de um requisito.

Eficácia

Medida em que as atividades planeadas são concretizadas e os resultados planeados atingidos.

Melhoria contínua

Atividade recorrente para melhorar o desempenho.

3 Principais conceitos e terminologia

Vulnerabilidades

Propriedades intrínsecas de algo que resultam na suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência.

Coordenador de exercícios

Pessoa responsável por planear, coordenar e implementar exercícios.

Observador

Participante que observa segmentos selecionados do exercício, à medida que estes se desenrolam, sem envolvimento nas atividades do exercício.

Monitorizar

Determinar o estado de um sistema, processo ou atividade.

Simulacro

Atividade que exercita uma competência particular e muitas vezes envolve repetição várias vezes.

Exercício

Processo para formar, avaliar, praticar e melhorar o desempenho numa organização.

Resposta a incidente

Ações realizadas, a fim de parar as causas do perigo iminente e mitigar as consequências de eventos potencialmente desestabilizadores ou disruptivos e recuperar para uma situação normal.

Comando de incidentes

Parte de uma estrutura organizada de para resposta a incidentes.

Comando e controlo

Atividades específicas, orientadas para uma meta, de tomada de decisão, avaliação da situação, planeamento, implementação de decisões e controlo dos efeitos da implementação durante o incidente.

Coordenação

Modo pelo qual diferentes organizações ou partes da mesma organização trabalham ou agem em conjunto para alcançar um objetivo comum.

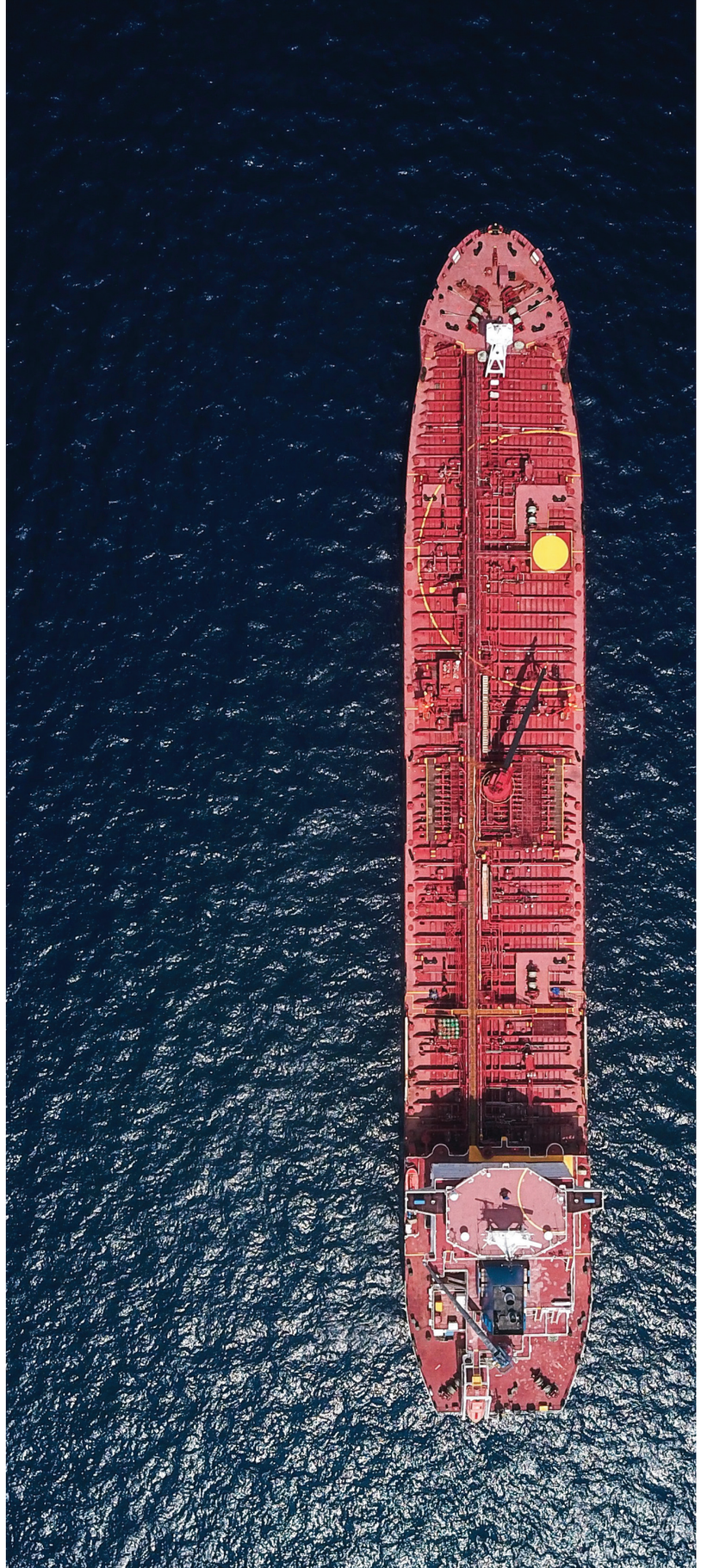
Proteção

Medidas que salvaguardem e habilitem uma organização a reduzir o impacto de uma potencial disrupção.

Recuperação

Restabelecimento e melhoria, quando apropriado, de operações, instalações, meios ou condições de vida de organizações afetadas, incluindo esforços para reduzir os fatores de risco.

Medidas tomadas para prevenir, limitar e reduzir o impacto das consequências negativas de incidentes, emergências e desastres.



Manual de Boas Práticas desenvolvido com base na norma ISO 28000

4 Pensamento baseado no Risco

O risco é inerente a todos os aspetos 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 atividades de planeamento, operação, análise e melhoria do Sistema de Gestão.

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:

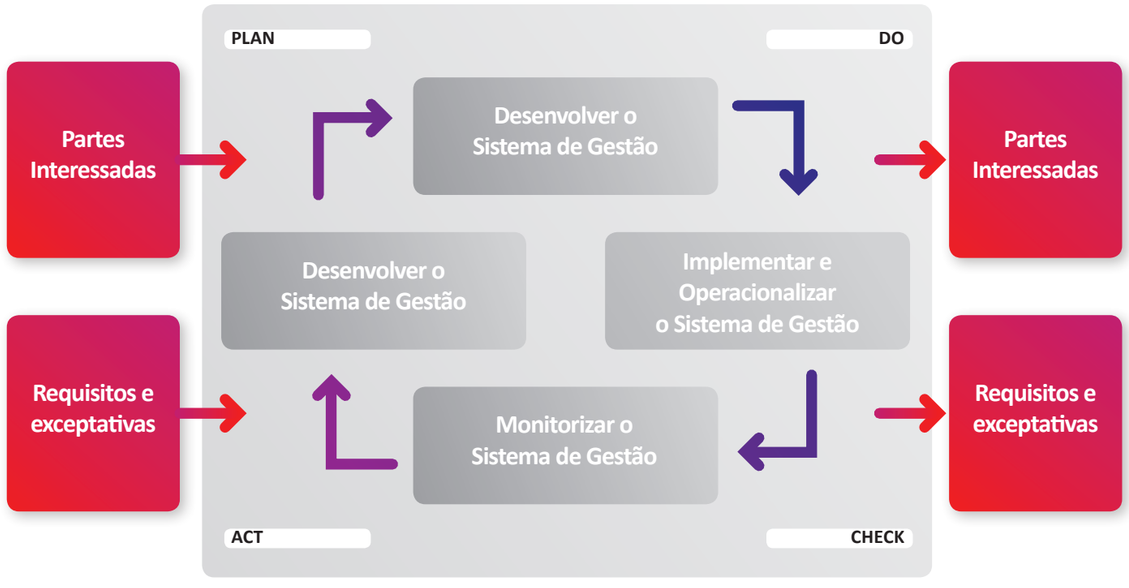
1. Plan (Planeamento)
Estabelecer objectivos, recursos necessários, requisitos das partes interessadas, políticas organizacionais e identificar risco e oportunidades.

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 modelo gráfico do PDCA é apresentado na figura seguinte:



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.

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

6

Metodologia de implementação

A metodologia para implementação consiste nos seguintes passos sequenciais, 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

6 Metodologia de Implementação

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

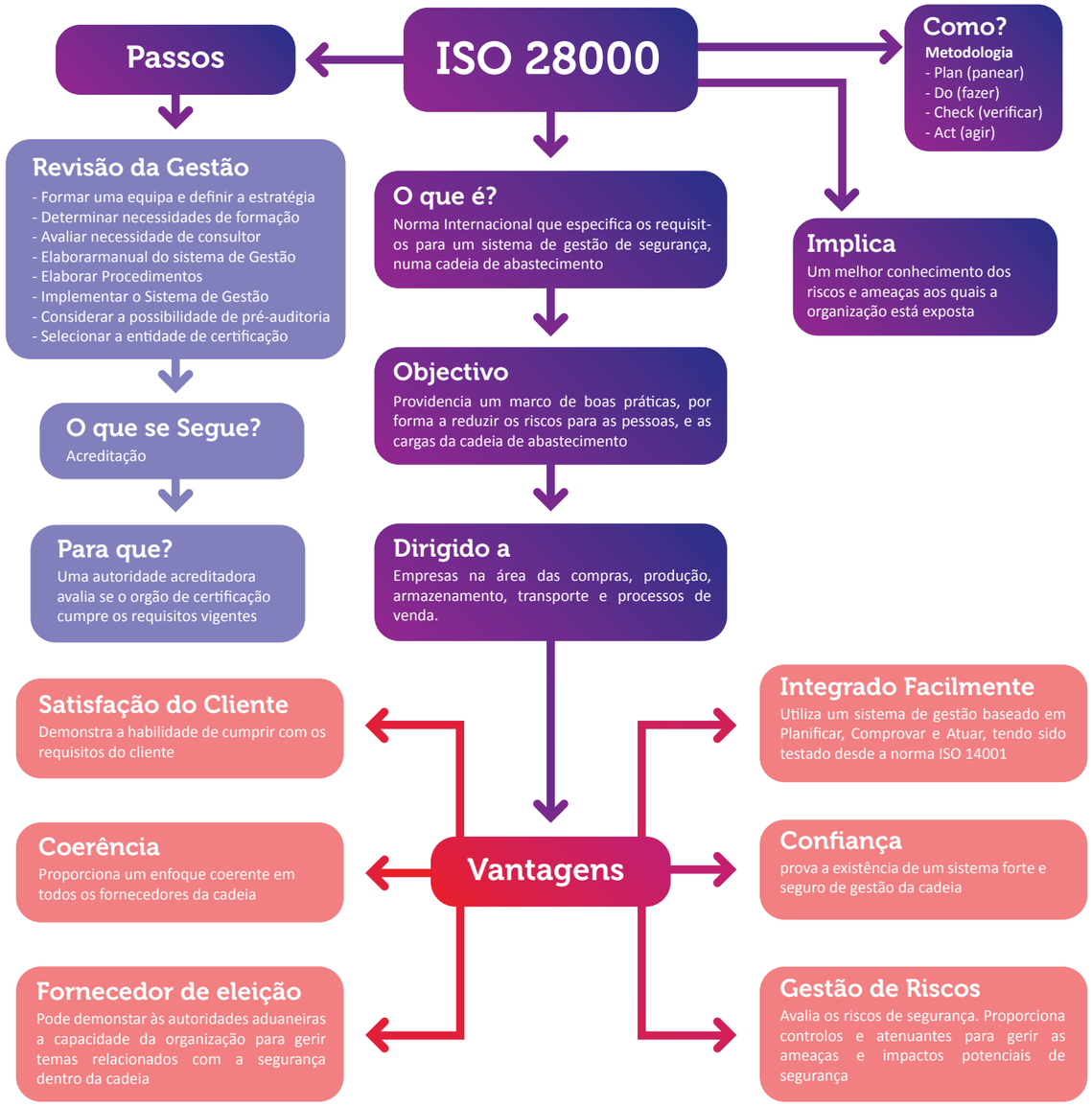
13. Auditoria de Certificação

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.

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

6 Metodologia de Implementação

O mapeamento geral da metodologia de implementação, incluindo resultados e impactes esperados, pode ser representado conforme figura seguinte.



7

Gestão Integrada

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/JJCG-TF 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.

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.

Anexo SL

A adoção do ISO Guide 83 – também conhecido por Anexo SL – serviu para a maior parte das normas de Sistema de Gestão com revisões recentes possuírem uma estrutura de requisitos similar, garantindo assim o alinhamento em organizações que possuem mais do que uma norma no seu Sistema de Gestão.

O anexo SL facilita a Gestão Integrada de uma sistema de gestão multi-norma, mas tal não é impeditivo para que um Sistema de Gestão Integrado com normas sem o Anexo SL.

O Anexo SL é composto por 10 clásulas:

- Objetivo e Campo de Aplicação
- Referências Normativas
- Termos e Definições
- Contexto da Organização
- Liderança
- Planeamento
- Suporte
- Operação
- Avaliação de Desempenho
- Melhoria

Destas cláusulas, o ponto de Termos e Definições não pode ser alterada. Requisitos não poderão ser removidos ou alterados, embora requisitos específicos possam ser adicionados.

Todos os Sistemas de Gestão implementados com base em normas que seguem o Anexo SL requerem que exista uma consideração do Contexto da Organização, um conjunto de Objetivos relevantes para a organização e alinhados com a estratégia da gestão de topo, uma Política Documentada para suportar a implementação do Sistema de Gestão e as suas metas, Auditorias internas para avaliar o grau de cumprimento com os requisitos e Revisão pela Gestão. Quando o Sistema de Gestão da organização está implementado segundo várias normas ISO, estes pontos podem ser combinados, se forma a serem realizados uma só vez, invés de múltiplas vezes.

8

Cláusulas normativas da ISO 28000 - Sistema de Gestão da Segurança da Cadeia de Abastecimento (SGSCA)

Requisitos gerais

A organização deve estabelecer, documentar, implementar, manter e melhorar continuamente um sistema eficaz de gestão da segurança para identificar ameaças de segurança, avaliar riscos e controlar e mitigar as suas consequências.

A organização deve melhorar continuamente a sua eficácia de acordo com os requisitos estabelecidos na Cláusula 4 da norma ISO 28000 e apresentados seguidamente.

Âmbito

A organização deve definir o âmbito do seu sistema de gestão da segurança. Quando a organização escolhe a subcontratação de processos que afetam a conformidade com estes requisitos, a organização deve assegurar que esses processos são controlados. Os controlos necessários e as responsabilidades por esses processos subcontratados devem ser identificados dentro do sistema de gestão da segurança.

Política de gestão da segurança

A gestão de topo da organização deve definir e aprovar uma política de gestão da segurança geral. A política deve:

- Ser consistente com outras políticas da organização;
- Disponibilizar uma estrutura que permita a elaboração de objetivos específicos da gestão da segurança, metas e programas;
- Ser consistente com a estrutura geral da organização para a gestão de riscos e ameaças de segurança;
- Ser adequada às ameaças da organização e à natureza e escala das suas operações;
- Definir claramente os objetivos gerais da gestão da segurança;
- Incluir o comprometimento para a melhoria continua do processo de gestão da segurança;
- Incluir o comprometimento para o cumprimento dos requisitos legais, regulatórios e estatutários vigentes aplicáveis e para outros requisitos subscritos pela organização;
- Ser visivelmente subscrita pela gestão de topo;
- Ser documentada, implementada e mantida;
- Ser comunicada a todos os colaboradores e terceiros relevantes, incluindo prestadores de serviços e visitantes com o objetivo de garantir que estas pessoas tomem conhecimento das suas obrigações individuais pela gestão da segurança;
- Estar disponível às partes interessadas sempre que apropriado;
- Providenciar a sua revisão em caso de aquisição ou fusão com outra organização, ou outra alteração ao âmbito do negocio da organização que possa afetar a continuidade ou relevância do sistema de gestão da segurança.

NOTA: As organizações podem escolher ter uma política detalhada da gestão da segurança para uso interno que poderá disponibilizar informação suficiente e diretrizes para conduzir o sistema de gestão da segurança (algumas partes podem ser confidenciais) e ter uma versão sumária (não confidencial) que contenha os objetivos alargados para disseminação a estas e outras partes interessadas.

8 Cláusulas normativas da ISO 28000

Apreciação e planeamento do risco de segurança

Apreciação do risco de segurança

A organização deve estabelecer e manter procedimentos para a identificação e avaliação contínua das ameaças de segurança e das ameaças e riscos relacionados com a gestão da segurança, e a identificação e implementação das medidas necessárias de gestão do controlo. Os métodos de identificação, avaliação e controlo de ameaças e riscos de segurança deverão, no mínimo, ser apropriados à natureza e escala das operações. Esta apreciação deve considerar a verosimilhança da ocorrência de um evento e todas as suas consequências que devem incluir:

- Ameaças e riscos das falhas físicas, como as falhas funcionais, danos acidentais, danos maliciosos ou atividades terroristas ou criminais;
- Ameaças e riscos operacionais, incluindo o controlo da segurança, fatores humanos e outras atividades que afetem a performance, o estado (ou condição?) ou a segurança (ou proteção?) da organização;
- Fenómenos naturais (tempestades, inundações, etc.), que poderão tornar ineficazes as medidas e equipamentos de segurança;
- Fatores fora do controlo da organização, como falhas de equipamentos e serviços fornecidos externamente;
- Ameaças e riscos das partes interessadas, como falhas no cumprimento de requisitos regulamentares ou danos na reputação ou na marca;
- Conceção e instalação de equipamento de segurança incluindo a substituição, manutenção, etc.;
- Informação e gestão de dados e comunicações;
- A ameaça à continuidade das operações.

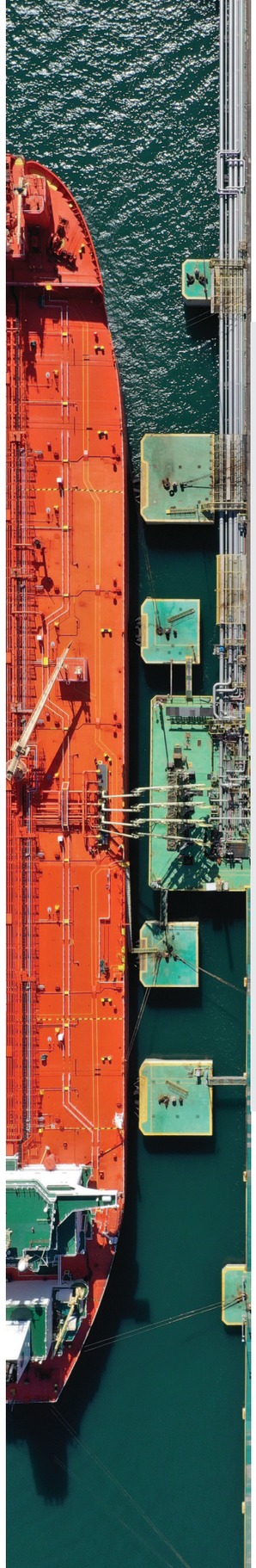
A organização deve garantir que os resultados destas avaliações e os efeitos destes controlos são considerados e, quando apropriado, disponibilizar entrada para:

- Objetivos e metas de gestão da segurança;
- Programas de gestão da segurança;
- A determinação de requisitos para a conceção, especificação e instalação;
- Identificação dos recursos adequados incluindo níveis de colaboradores;
- Identificação das necessidades de formação e competências (ver competência, formação e consciencialização);
- Desenvolvimento de controlos operacionais (ver controlo operacional);
- Estrutura global de gestão de ameaça e risco da organização.

A organização deve documentar e manter atualizada a informação acima referida.

A metodologia da organização para a identificação e apreciação da ameaça e do risco deve:

- Ser definida de acordo com o seu âmbito, natureza e calendarização para assegurar que é proativa em vez de reativa;
- Incluir o conjunto de informação relacionada com ameaças e riscos de segurança;
- Providenciar a classificação de ameaças e riscos e identificar aqueles que devem ser evitados, eliminados ou controlados;
- Providenciar a monitorização de ações que garantam a eficácia e a oportunidade da sua implementação (ver monitorização e medição).



Manual de Boas Práticas desenvolvido com base na norma ISO 28000

8 Cláusulas normativas da ISO 28000

A metodologia para a apreciação do risco, segue de base a norma ISO 31000 sendo adaptada tendo por base os alvos em apreciação:

A definição de Contramedidas é função da Probabilidade e da Consequência da ocorrência de um dado cenário, devendo seguir-se a metodologia apresentada nas normas ISO 28001 e ISO 20858, que se apresenta na imagem seguinte.

		Consequência		
		Alta	Média	Baixa
Probabilidade	Alta	contramedidas	contramedidas	
	Média	contramedidas		
	Baixa			

8 Cláusulas normativas da ISO 28000

Requisitos legais, estatutários e outros requisitos regulamentares de segurança

A organização deve estabelecer, implementar e manter um procedimento:

- Para identificar e ter acesso aos requisitos legais aplicáveis e outros requisitos que a organização subscreva em relação às suas ameaças e riscos de segurança, e
- Para determinar como estes requisitos se aplicam às suas ameaças e riscos de segurança.
- A organização deve manter esta informação atualizada. Deve comunicar informação relevante legal e outros requisitos aos seus colaboradores e a outras terceiras partes relevantes, incluindo subcontratados.

Objetivos de gestão da segurança

A organização deve estabelecer, implementar e manter documentado os objetivos de gestão da segurança para as funções e níveis relevantes dentro da organização. Os objetivos devem resultar e serem consistentes com a política. No momento da definição e da revisão dos seus objetivos, a organização deve ter em consideração:

- Requisitos legais, estatutários e outros requisitos regulamentares de segurança;
- Ameaças e riscos relacionados com a segurança;
- Tecnológico e outras opções;
- Requisitos financeiros, operacionais e de negócio;
- Pontos de vista das adequadas partes interessadas;

Os objetivos de gestão da segurança devem ser:

- Consistentes com o comprometimento da organização quanto à melhoria continua;
- Quantificáveis (quando praticável);
- Comunicados a todos os colaboradores e terceiras partes relevantes, incluindo subcontratados, com a intenção que estas pessoas estejam conscientes das suas obrigações individuais;
- Revistos periodicamente para assegurar que se mantêm relevantes e consistentes com a política de gestão da segurança. Sempre que necessário os objetivos de gestão da segurança devem ser alterados em conformidade.

Metas de gestão da segurança

A organização deve estabelecer, implementar e manter documentado as metas de gestão da segurança apropriadas às necessidades da organização. As metas devem resultar e ser consistentes com os objetivos de gestão da segurança.

Estas metas devem ser:

- De um nível de detalhe apropriado;
- Especificas, mensuráveis, atingíveis, relevantes e time-based (quando praticável);
- Comunicadas a todos os colaboradores e terceiras partes relevantes incluindo subcontratados com objetivo de que estes indivíduos passem a ter consciência das suas obrigações individuais;
- Revistas periodicamente para assegurar que se mantêm relevantes e consistentes com os objetivos de gestão da segurança. Quando necessário as metas devem ser alteradas em conformidade.

Programas de gestão da segurança

A organização deve estabelecer, implementar e manter programas de gestão da segurança para atingir os objetivos e metas. Os programas devem ser otimizados e posteriormente priorizados, e a organização deve assegurar a implementação eficiente e rentável destes programas. Isto deve incluir documentação que descreva:

- A responsabilidade e a autoridade designadas para atingir os objetivos e metas de gestão da segurança;
- Os meios e a escala temporal através dos quais os objetivos e metas de gestão da segurança poderão ser atingidos.
- Os programas de gestão da segurança devem ser revistos periodicamente para garantir que se mantém efetivos e consistentes com os objetivos e metas. Quando necessário os programas devem ser alterados em conformidade.

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

8 Cláusulas normativas da ISO 28000

Implementação e operacionalização

Estrutura, autoridade e responsabilidades para a gestão da segurança

A organização deve estabelecer e manter uma estrutura organizacional de funções, responsabilidades e autoridades, coerente com a consecução da sua política de gestão da segurança, dos seus objetivos, das suas metas e dos seus programas. Estas funções, responsabilidades e autoridades devem ser definidas, documentadas e comunicadas aos indivíduos responsáveis pela implementação e manutenção.

A gestão de topo deve fornecer evidências do seu empenho no desenvolvimento e implementação do sistema de gestão da segurança (processos) e melhorar continuamente a sua eficácia ao:

- Nomear um membro da gestão de topo que, independentemente de outras responsabilidades, deve ser responsável pela conceção global, manutenção, documentação e melhoria do sistema de gestão da segurança da organização;
- Nomear o(s) membro(s) da gestão com a autoridade necessária para assegurar a implementação dos objetivos e metas;
- Identificar e monitorizar os requisitos e expectativas das partes interessadas da organização e tomar as medidas apropriadas e oportunas para gerir estas expectativas;
- Assegurar a disponibilidade dos recursos adequados;
- Considerar o impacto adverso que a política de gestão de segurança, os objetivos, as metas, os programas, etc. poderão ter sobre outros aspetos da organização;
- Assegurar que quaisquer programas de segurança gerados a partir de outras partes da organização complementam o sistema de gestão da segurança;
- Comunicar à organização a importância da observância dos seus requisitos de gestão da segurança por forma a cumprir a sua política;
- Assegurar que as ameaças e riscos relacionados com a segurança são avaliados e incluídos nas apreciações de ameaça e de risco da organização, conforme for apropriado;
- Assegurar a viabilidade dos objetivos, metas e programas de gestão da segurança.

Competência, formação e consciencialização

A organização deve assegurar que o pessoal responsável pela conceção, operação e gestão dos equipamentos e processos de segurança seja devidamente qualificado em termos de educação, formação e / ou experiência. A organização deve estabelecer e manter procedimentos para que as pessoas que trabalham para ela ou em seu nome, estejam cientes:

- Da importância do cumprimento da política e procedimentos de gestão da segurança e dos requisitos do sistema de gestão da segurança;
- Das suas funções e responsabilidades na consecução do cumprimento da política e dos procedimentos de gestão da segurança e dos requisitos do sistema de gestão da segurança, incluindo os requisitos da preparação e resposta a emergências;
- Das consequências potenciais para a segurança da organização no caso de não se seguirem os procedimentos operacionais especificados.

Devem ser mantidos registos da competência e da formação.

8 Cláusulas normativas da ISO 28000

Comunicação

A organização deve dispor de procedimentos para garantir que a informação de gestão da segurança pertinente seja comunicada a colaboradores, subcontratados e outras partes interessadas relevantes.

Devido à natureza sensível de certas informações relacionadas com a segurança, deverá ser dada a devida consideração à sensibilidade da informação antes da disseminação.

Documentação

A organização deve estabelecer e manter um sistema de documentação de gestão da segurança que inclua, mas não se limite ao seguinte:

- À política da segurança, objetivos e metas;
- Descrição do âmbito do sistema de gestão da segurança;
- Descrição dos principais elementos do sistema de gestão da segurança e sua interação, e referência a documentos relacionados;
- Documentos, incluindo registos, exigidos pela presente Norma Internacional;
- Documentos, incluindo os registos determinados pela organização, necessários para garantir o efetivo planeamento, operacionalização e controlo de processos que se relacionam com as suas ameaças e riscos significativos de segurança.

A organização deve determinar a sensibilidade da segurança de informação (ou, da informação de segurança?) e deve tomar medidas para prevenir o acesso não autorizado.

Controlo de documentos e dados

A organização deve estabelecer e manter procedimentos para controlar todos os documentos, dados e informações exigidas pela Cláusula 4 da presente Norma para garantir que:

- Estes documentos, dados e informações podem ser localizados e acedidos apenas por indivíduos autorizados;
- Estes documentos, dados e informações são periodicamente revistos, conforme necessário, e aprovada a adequação por pessoal autorizado;
- As versões atuais de documentos, dados e informações relevantes estão disponíveis em todos os locais onde as operações essenciais para o funcionamento efetivo do sistema de gestão da segurança são realizadas;
- Documentos obsoletos, dados e informações são imediatamente removidos de todos os pontos de emissão e pontos de utilização, ou de outra forma assegurados contra o uso indesejado;
- Documentos de arquivo, dados e informações retidos para fins legais ou de preservação do conhecimento ou ambos são devidamente identificados;
- Estes documentos, dados e informações estão seguros, e se em formato eletrónico são adequadamente copiados (protegidos ou reforçados?) e podem ser recuperados.

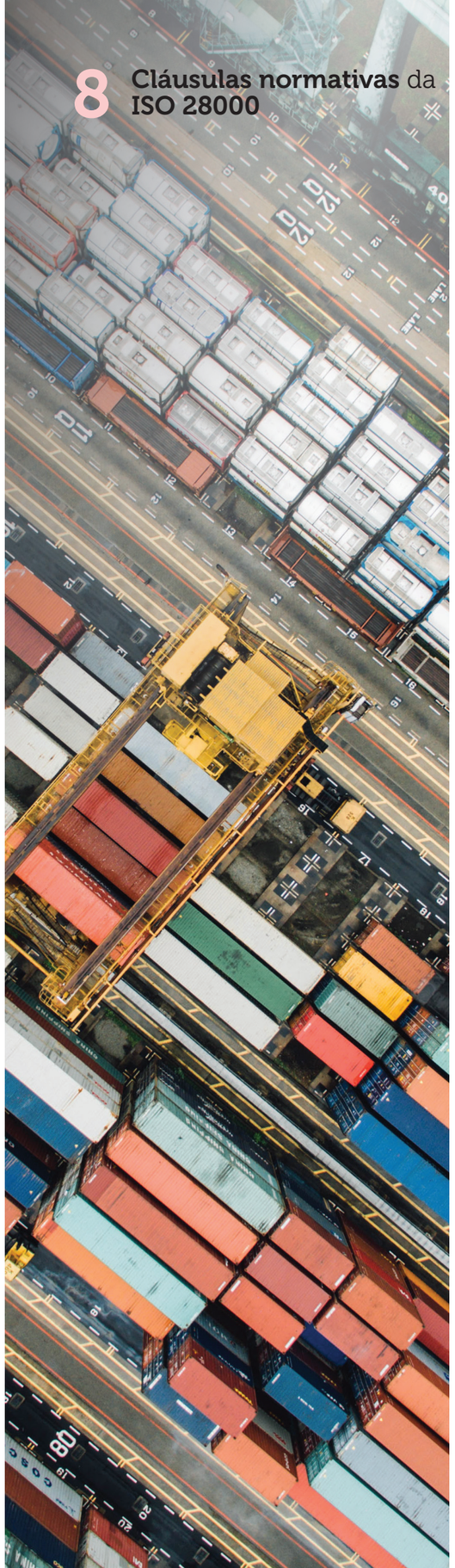
Controlo operacional

A organização deve identificar as operações e atividades necessárias para atingir:

- A sua política de gestão da segurança;
- O controlo de atividades e mitigação de ameaças identificadas como tendo risco significativo;
- Conformidade com requisitos legais, estatutários e outros requisitos regulamentares de segurança;
- Os seus objetivos de gestão da segurança;
- A execução dos seus programas de gestão da segurança;
- O nível requerido de segurança da cadeia de fornecimento.

A organização deve assegurar que estas operações e atividades sejam levadas a cabo sob condições especificadas:

- Estabelecendo, implementando e mantendo procedimentos documentados para controlar situações onde a sua ausência poderá conduzir à falha na prossecução das operações e atividades listadas nas alíneas a) a f) do requisito 4.4.6, acima mencionado;
- Avaliando quaisquer ameaças decorrentes de atividades a montante da cadeia de fornecimento e aplicando controlos para mitigar esses impactos para a organização e outros operadores a jusante da cadeia de fornecimento;
- Estabelecendo e mantendo os requisitos para mercadorias ou serviços com impacto na segurança e comunicando-os a fornecedores e contratados.



8 Cláusulas normativas da ISO 28000

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

Estes procedimentos devem incluir controlos para a conceção, instalação, operação, remodelação, e modificação de itens de equipamentos, instrumentação, etc. relacionados com a segurança, conforme apropriado. Quando as disposições existentes são revistas ou novas disposições são introduzidas, que possam criar impacto nas operações e atividade de gestão da segurança, a organização deve considerar as ameaças e riscos associados antes da sua implementação. As novas ou revistas disposições/combinações a ser consideradas devem incluir:

- Estrutura organizacional, funções ou responsabilidades, revistas;
- Política da gestão da segurança, objetivos, metas ou programas, revistos;
- Processos e procedimentos revistos;
- Introdução de nova infraestrutura, equipamento ou tecnologia de segurança, que poderão incluir hardware e/ou software;
- A introdução de novos subcontratados, fornecedores ou pessoal, conforme apropriado.

Preparação da emergência, resposta e recuperação da segurança

A organização deve estabelecer, implementar e manter planos e procedimentos adequados para identificar o potencial para, e respostas a incidentes de segurança e situações de emergência, prevenindo e mitigando as consequências prováveis que podem ser associadas aos mesmos. Os planos e procedimentos devem incluir informações sobre o fornecimento e manutenção de qualquer equipamento, instalações ou serviços identificados que podem ser necessários durante ou após os incidentes ou situações de emergência.

A organização deve periodicamente rever a eficácia da sua preparação da emergência, resposta e planos e procedimentos de recuperação da segurança, em particular após a ocorrência de incidentes ou situações de emergência causadas por violações e ameaças de segurança. A organização deve testar periodicamente estes procedimentos quando praticável.

Deverá ser dada a devida consideração à sensibilidade da informação antes da disseminação.

8 Cláusulas normativas da ISO 28000

Verificação e ação corretiva

Monitorização e medição do desempenho da segurança

A organização deve estabelecer e manter procedimentos para monitorizar e medir o desempenho do seu sistema de gestão da segurança. A organização deve ainda estabelecer e manter procedimentos para monitorizar e medir o desempenho da segurança. A organização deve considerar as ameaças e riscos à segurança, incluindo mecanismos de potencial deterioração e suas consequências, aquando do estabelecimento da frequência de medição e monitorização dos parâmetros-chave do desempenho. Estes procedimentos devem prever:

- Medições qualitativas e quantitativas apropriadas às necessidades da organização;
- Monitorização do grau de cumprimento da política, objetivos e metas;
- Medidas proactivas de desempenho da monitorização da conformidade com o(s) programa(s) de gestão da segurança, critérios de controlo operacional, legislação aplicável e outros requisitos estatutários e regulamentares;
- Medidas reativas de desempenho para monitorizar as deteriorações, falhas, incidentes e não-conformidades relacionadas com a segurança (incluindo os quase acidentes e falsos alarmes) e outra evidência histórica de desempenho deficiente do sistema de gestão da segurança;
- Registo dos dados e resultados da monitorização e medição, suficiente para facilitar a análise das ações corretivas e preventivas subsequentes. Se for necessário dispor de equipamento de monitorização ou medição, a organização deve providenciar o estabelecimento e manutenção de procedimentos para a calibração e manutenção desse equipamento. Os registos das atividades e dos resultados de calibração e manutenção devem ser mantidos o tempo suficiente para cumprir com a legislação e com a política da organização.

Avaliação do sistema

A organização deve avaliar os planos, procedimentos e capacidade da gestão da segurança através de revisões, testes, relatórios pós-incidentes, lições aprendidas, avaliações do desempenho e exercícios, periódicos. Alterações significativas nestes fatores deverão ser de imediato refletidas no(s) procedimento(s).

A organização deve avaliar periodicamente o cumprimento da legislação, dos regulamentos e boas práticas do setor, bem como a conformidade com a sua política e objetivos.

A organização deve manter os registos dos resultados das avaliações periódicas.

Falhas, incidentes, não conformidades e ação corretiva e preventiva relacionados com a segurança

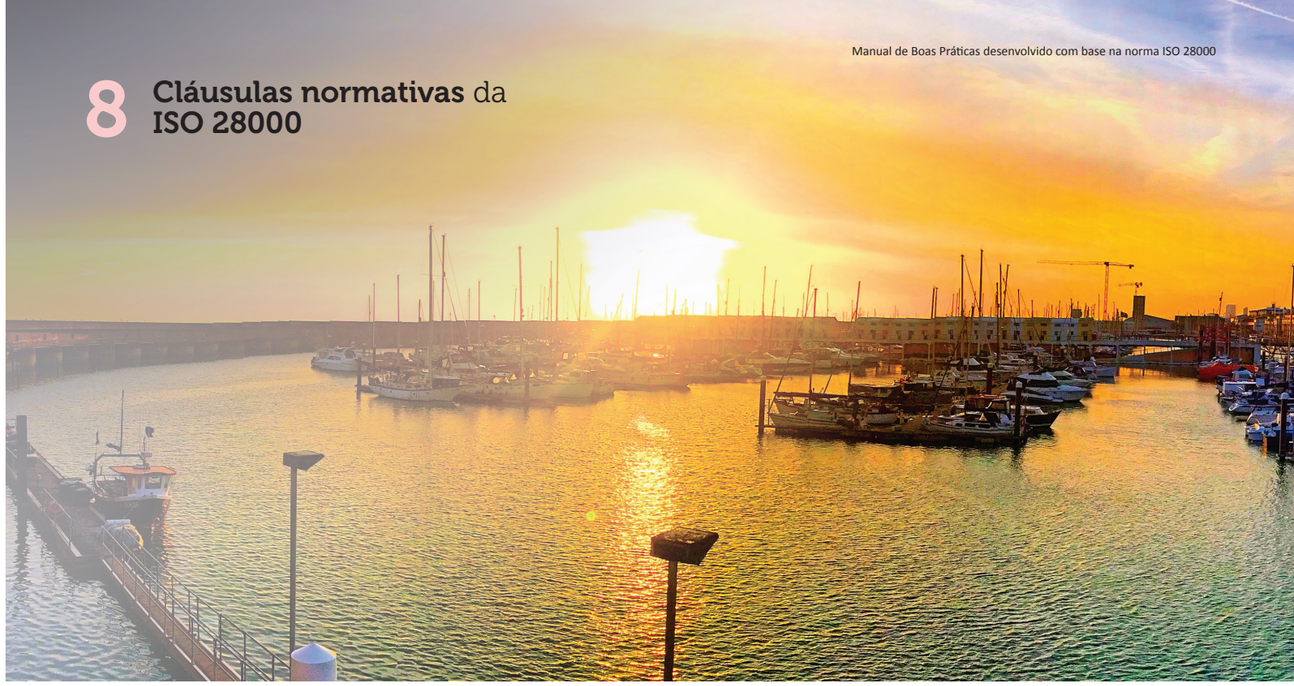
A organização deve estabelecer, implementar e manter procedimentos para definir responsabilidade e autoridade para:

- Avaliar e iniciar ações preventivas para identificar potenciais falhas de segurança, a fim de prevenir a sua ocorrência;
- A investigação relacionada com a segurança:
  1. Falhas incluindo quase acidentes e falsos alarmes;
  2. Incidentes e situações de emergência;
  3. Não conformidades;
- Tomada de ação para mitigar quaisquer consequências decorrentes de tais falhas, incidentes ou não conformidades;
- A iniciação e conclusão de ações corretivas;
- A confirmação da eficácia das ações corretivas definidas;

Estes procedimentos devem requerer que as ações corretivas e preventivas propostas são revistas através do processo de apreciação do risco e ameaça da segurança antes da implementação, a menos que a imediata implementação previna exposições para a vida ou segurança (ou proteção) pública.

Qualquer ação corretiva ou preventiva definida para eliminar as causas das atuais e potenciais não conformidades deve ser apropriada à magnitude dos problemas e proporcional às ameaças e riscos relacionadas com a segurança que, provavelmente, se deparem. A organização deve implementar e registar quaisquer alterações aos procedimentos documentados, resultantes das ações corretivas e preventivas e deve incluir a formação adequada sempre que necessário.

8 Cláusulas normativas da ISO 28000



Controlo dos registos

A organização deve estabelecer e manter os registos necessários para demonstrar a conformidade com os requisitos do seu sistema de gestão da segurança e da presente norma, e os resultados obtidos.

A organização deve estabelecer, implementar e manter um ou mais procedimentos para a identificação, arquivo, proteção, recuperação, retenção e eliminação dos registos. Os registos devem ser e permanecer legíveis, identificáveis e rastreáveis.

A documentação eletrónica e digital deverá manter a sua integridade preservada, com cópia de segurança e apenas acessível a pessoal autorizado.

Auditoria

A organização deve estabelecer, implementar e manter um programa de gestão de auditorias e deve assegurar que as auditorias ao sistema de gestão da segurança sejam realizadas a intervalos planeados, visando:

- Determinar ou não se o sistema de gestão da segurança:
  1. Está conforme com as disposições planeadas para a gestão da segurança, incluindo os requisitos da cláusula 4 desta especificação;
  2. Tem sido apropriadamente implementado e mantido;
  3. É (são) eficaz(es) no cumprimento da política e objetivos de gestão da segurança da organização;
- Rever os resultados de auditorias anteriores e das ações definidas para retificar não conformidades;
- Disponibilizar informação dos resultados das auditorias, à gestão;
- Verificar que o equipamento e pessoal da segurança são apropriadamente empregues.

O programa de auditorias deve basear-se nos resultados das apreciações do risco e da ameaça das atividades da organização, e nos resultados de auditorias anteriores. Os procedimentos de auditoria devem definir o âmbito, frequência, metodologias e competências, bem como responsabilidades e requisitos para condução das auditorias e reportar os resultados. Sempre que possível, as auditorias devem ser conduzidas por pessoal independente das atividades a serem auditadas.

NOTA a frase “pessoal independente” não significa necessariamente pessoal externo à organização.

Revisão pela gestão e melhoria contínua

A gestão de topo deve rever o Sistema de Gestão da Segurança, em intervalos planeados, para assegurar o seu ajustamento, adequação e eficácia contínuos. As revisões devem incluir a avaliação das oportunidades para melhoria e a necessidade de alterações ao Sistema de Gestão da Segurança, incluindo a política de segurança, objetivos da segurança e ameaças e riscos. Os registos da revisão pela gestão devem ser mantidos. As entradas para a revisão pela gestão devem incluir:

- Resultados de auditorias e avaliações da conformidade com os requisitos legais e com outros requisitos que a organização subscreva;
- Comunicações das partes interessadas externas, incluindo reclamações;
- Desempenho da segurança da organização;
- O grau de cumprimento dos objetivos e metas;
- Estado das ações corretivas e das ações preventivas;
- Ações de seguimento resultantes de anteriores revisões pela gestão;
- Alterações de circunstâncias, incluindo desenvolvimentos nos requisitos legais e outros requisitos relacionados com a segurança;
- Recomendações para melhoria.

As saídas das revisões pela gestão devem incluir quaisquer decisões e ações relacionadas com possíveis alterações à política de segurança, objetivos, metas e outros elementos do Sistema de Gestão da Segurança, consistente com o compromisso com a melhoria contínua.

Manual de Boas Práticas desenvolvido com base na norma ISO 28000

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.

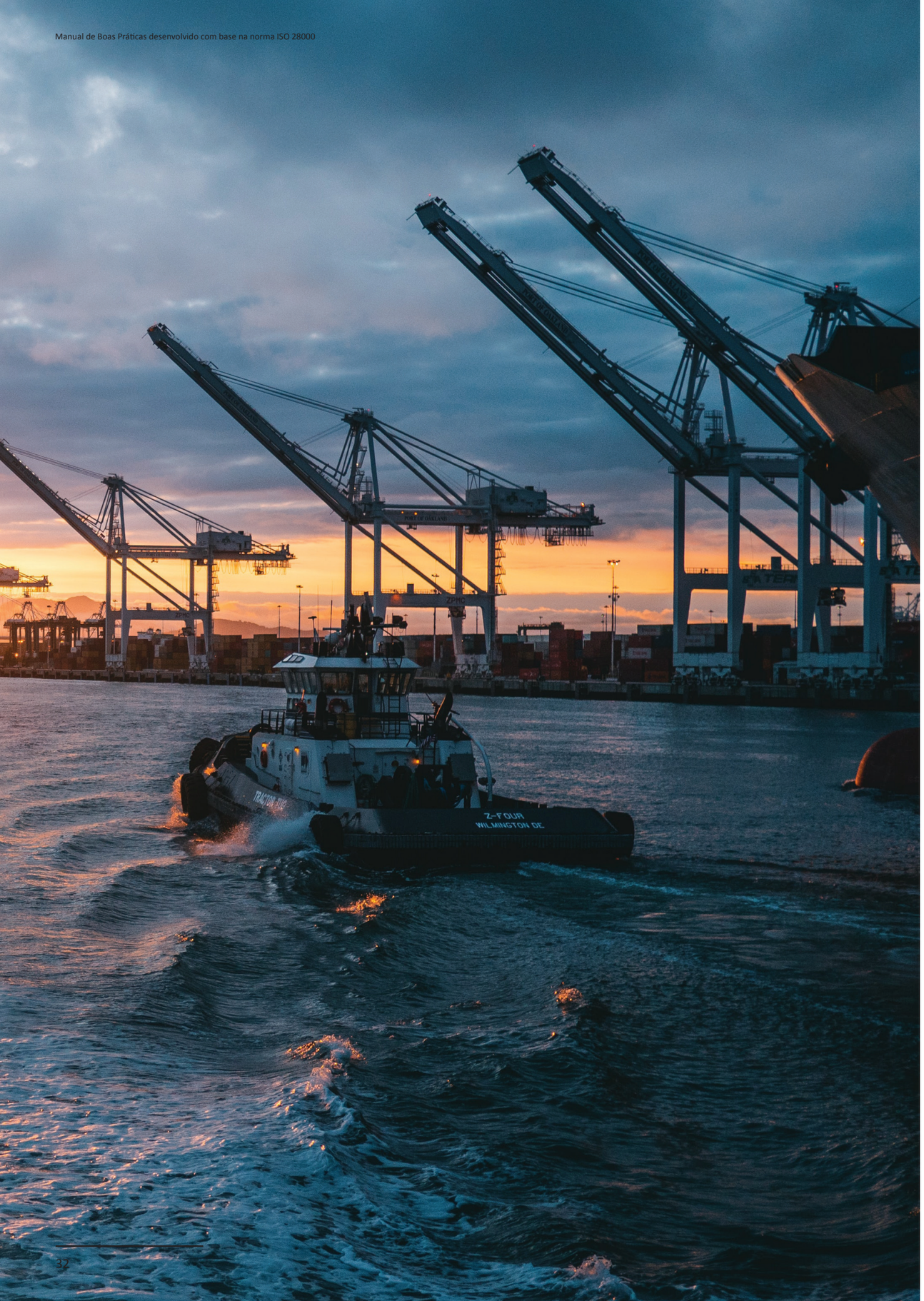
O processo de certificação tem por base a Auditoria de Certificação. As auditorias de concessão são realizadas em 2 fases distintas. Na 1ª fase da auditoria, a equipa auditora tem a oportunidade de ter um primeiro contacto com a organização auditada e efetuar uma avaliação prévia da sua estrutura organizacional 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).



10
Referências

1. *ISO 28001 - Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective;*
2. *ISO 28003 - Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems;*
3. *ISO 28004 - Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective;*
4. *ISO 9001 - Quality management systems — Requirements;*
5. *ISO 20858 - Ships and marine technology — Maritime port facility security assessments and security plan development;*
6. *ISO 22300 - Security and resilience — Vocabulary;*
7. *ISO 31000 – Risk Management – Principles and Guidelines;*
8. *ISO Guide 73, Risk management — Vocabulary;*
9. *SAFE Framework of Standards – Appendix to Annex 1, World Customs Organization;*

11 Anexos

ISO 28000:2007		ISO 27001:2013		ISO 9001:2015	
Requisitos do sistema de gestão da segurança da cadeia de abastecimento (somente título	4	• Contexto da organização (somente título) • Compreender a organização e o seu contexto • Compreender as necessidades e expectativas das partes interessadas	4. 4.1 4.2	• Contexto da organização (somente título) • Compreender a organização e o seu contexto • Compreender as necessidades e expectativas das partes interessadas	4. 4.1 4.2
Requisitos Gerais	4.1	• Determinar o âmbito do sistema de gestão da segurança da informação • Sistema de Gestão da Segurança da Informação • Melhoria Contínua	4.3 4.4 10.3	• Determinar o âmbito do sistema de gestão da Qualidade • Sistema de Gestão da Qualidade • Melhoria Contínua	4.3 4.4 10.3
Política de gestão da segurança	4.2	Política	5.2	Política	5.2
Apreciação e planeamento do risco de segurança (somente título)	4.3	• Planeamento (somente título) • Ações para endereçar riscos e oportunidades • Generalidades • Avaliação do risco de segurança da informação • Tratamento do risco de segurança da informação	6 6.1 6.1.1 8.2 8.3	• Planeamento (somente título) • Ações para tratar riscos e oportunidades	6 6.1
Apreciação do risco de segurança	4.3.1	• Avaliação do risco de segurança da informação • Tratamento do risco de segurança da informação	6.1.2 6.1.3	• Ações para tratar riscos e oportunidades	6.1
Requisitos legais, estatutários e outros requisitos regulamentares de segurança	4.3.2	Tratamento do risco de segurança da informação	6.1.3	Requisitos para produtos e serviços	8.2
Objetivos de gestão da segurança	4.3.3	Objectivos de segurança da informação e planeamento para os alcançar	6.2	Objetivos da qualidade e planeamento para os atingir	6.2
Metas de gestão da segurança	4.3.4	Objectivos de segurança da informação e planeamento para os alcançar	6.2	Objetivos da qualidade e planeamento para os atingir	6.2
Programas de gestão da segurança	4.3.5	Objectivos de segurança da informação e planeamento para os alcançar	6.2	Objetivos da qualidade e planeamento para os atingir	6.2
Implementação e operacionalização (somente título)	4.4	• Suporte (somente título) • Operação (somente título) • Liderança (somente título)	7 8 5	• Suporte (somente título) • Operacionalização (somente título) • Liderança (somente título)	7 8 5
Estrutura, autoridade e responsabilidades para a gestão da segurança	4.4.1	• Recursos • Funções, responsabilidades e autoridades na organização • Liderança e comprometimento	7.1 5.3 5.1	• Recursos • Funções, responsabilidades e autoridades organizacionais • Liderança e compromisso	7.1 5.3 5.1
Competência, formação e consciencialização	4.4.2	• Competência • Consciencialização	7.2 7.3	• Competências • Consciencialização	7.2 7.3
Comunicação	4.4.3	Comunicação	7.4	Comunicação	7.4
Documentação	4.4.4	Informação documentada	7.5	Informação documentada	7.5

ISO 28000:2007		ISO 27001:2013		ISO 9001:2015	
Controlo de documentos e dados	4.4.5	• - Criação e atualização • - Controlo da informação documentada	7.5.2 7.5.3	• - Criação e atualização • - Controlo da informação documentada	7.5.2 7.5.3
Controlo operacional	4.4.6	• - Planeamento e controlo operacional • - Tratamento do risco de	8.1 8.3	• - Planeamento e controlo operacional	8.1
Preparação da emergência, resposta e recuperação da segurança	4.4.7	Avaliação do risco de segurança da informação	8.2	- Requisitos para produtos e serviços	8.2
Verificação e ação corretiva (somente título)	4.5	• Avaliação de desempenho (somente título)	9	• Avaliação de desempenho (somente título)	9
Monitorização e medição do desempenho da segurança	4.5.1	• Monitorização, medição, análise e avaliação	9.1	• - Monitorização, medição, análise e avaliação • - Generalidades	9.1 9.1.1
Avaliação do sistema	4.5.2	Auditoria interna	9.2	Análise e Avaliação	9.1.3
Falhas, incidentes, não conformidades e ação corretiva e preventiva relacionados com a segurança	4.5.3	Não conformidade e ação cor	10.1	Não conformidade e ação correctiva	10.2
Controlo dos registos	4.5.4	Controlo da informação docu	7.5.3	Controlo da informação documentada	7.5.3
Auditoria	4.5.5	Auditoria interna	9.2	Auditoria interna	9.2
• - Revisão pela Gestão • - Melhoria contínua	4.6	• - Revisão pela Gestão • - Melhoria contínua	9.3 10.2	• - Revisão pela Gestão • - Melhoria contínua	9.3 10.3

Este manual é propriedade da Qualiseg - Engenharia e Gestão Lda., está interdita qualquer cópia ou distribuição sem autorização expressa da mesma.