QUALIseg
ENGENHARIA E GESTÃO, LDA.

GISAMP

ISO 28 000 - Sistema de Gestão de Segurança para a Cadeia de Abastecimento

requisitos da ISO 28000

Cofinanciado por:

REPÚBLICA PORTUGUESA
MAR

fundoazul

4.1 Requisitos gerais

- A organização deve estabelecer, documentar, implementar, manter e melhorar de maneira contínua um SGSCA eficaz para identificar **ameaças** de segurança, avaliar os **riscos** e controlar e mitigar suas **consequências**.
- A organização deve definir o **âmbito** do seu SGSCA.
- Deve-se assegurar que os **processos contratados externamente cumpram** com os requisitos do SGSCA.

4.2 Política de gestão de segurança

- A gestão de topo da organização deve autorizar uma **politica de gestão de segurança global**. A politica deve:
  - Ser consistente com **outras políticas** da organização.
  - Proporcionar estrutura que permita alcançar os **objetivos**, as metas e os programas específicos de gestão de segurança.
  - Ser **consistente** com a estrutura global de gestão de riscos e de ameaças da organização
  - Ser **apropriada** para tratar as **ameaças** a organização e a natureza e dimensão de suas **operações**
  - Incluir o compromisso com a **melhoria contínua** do processo de gestão de segurança.

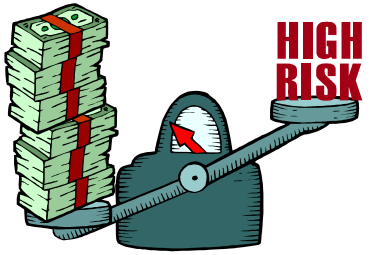
4.2 Política de gestão de segurança

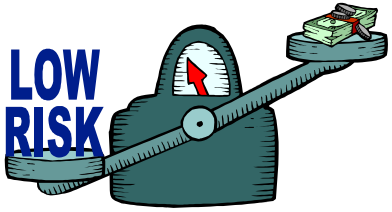
- Incluir o compromisso de **cumprir a legislação** vigente aplicável, requisitos regulamentares/legais e outros requisitos aos quais a organização esta subordinada
- Estar claramente **assumida** pela gestão de topo
- Estar **documentada**, implementada e atualizada
- **Comunicada** a todos os colaboradores e terceiros pertinentes, bem como estar disponível
- Providenciar a sua **revisão** no caso de aquisição ou fusão com outras organizações ou outra mudança no âmbito do negócio da organização que possa afetar a continuidade do SGSCA
- *Pode existir uma **política confidencial** que ofereça informações e instruções suficientes para conduzir o SGSCA e uma outra resumida (não confidencial) para divulgação ao público e partes interessadas.*

4.3.1 Avaliação do risco de segurança

- A organização deve estabelecer e manter procedimentos para a **identificação e avaliação permanente de ameaças** à segurança e **riscos** relacionados a gestão de segurança assim como a identificação e implementação das **medidas de controlo** necessárias.

- Os métodos de identificação, avaliação e controlo de ameaças e riscos à segurança, devem pelo menos ser apropriados à natureza e escala das operações.





4.3.1 Avaliação do risco de segurança

A avaliação de riscos deve incluir:

- Ameaças e riscos **materiais/equipamentos**, tais como falha funcional, dano incidental, dano intencional ou ato terrorista e criminal
- Ameaças e riscos **operacionais**
- Eventos da **natureza** (tempestade, enchentes, etc.) que possam tornar ineficientes as medidas e equipamentos de segurança, incluindo fatores humanos
- Fatores fora do controlo da organização, tais como **falhas** de equipamentos/serviços fornecidos externamente
- **Ameaças e riscos** das partes interessadas, tais como falhas no cumprimento de requisitos regulamentares ou danos na reputação ou na marca
- Projeto e instalação de **equipamentos de segurança**, incluindo substituição, manutenção, etc...
- Gestão de **dados**, informação e comunicações
- Ameaças à **continuidade** das operações.

4.3.1 Avaliação do risco de segurança

Os resultados da avaliação de riscos deverão proporcionar a seguinte informação:

- **Objetivos e metas** de gestão de segurança
- **Programas de gestão** de segurança
- Determinação de **requisitos** para a conceção, especificação e instalação
- Identificação dos **recursos** adequados, incluindo níveis de colaboradores
- Identificação das necessidades de **formação e competência** (ver 4.4.2)
- Desenvolvimento dos **controlos operacionais** (ver 4.4.6)
- Estrutura global de gestão de **ameaça e risco** da organização.

4.3.1 Avaliação do risco de segurança

A avaliação de riscos e seus resultados deverá ser documentada e mantida atualizada permanentemente

4.3.1 Avaliação do risco de segurança

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

a) ser definida de acordo com o seu âmbito, natureza e calendarização para assegurar que é **proativa** em vez de reativa;

b) incluir o conjunto de informação relacionada com **ameaças e riscos** de segurança;

c) providenciar a **classificação** de ameaças e riscos e identificar aqueles que devem ser evitados, eliminados ou controlados;

d) providenciar a **monitorização** de ações que garantam a eficácia e a oportunidade da sua implementação (ver 4.5.1).

Metodologia: Gestão de Riscos

- A metodologia deverá considerar a seguinte sequência:

a) Lista de todas as atividades do **ÂMBITO**

b) Identificação dos **CONTROLOS EXISTENTES** na **ATUALIDADE**

c) Identificação dos **CENÁRIOS** de **AMEAÇAS**

d) Determinar as **CONSEQUÊNCIAS** derivadas caso uma **AMEAÇA** se materialize num **CENÁRIO**

e) Cálculo de probabilidade/verosimilhança de que isto ocorra tendo em conta o nível de **SEGURANÇA ATUAL**

f) Estimativa **ADEQUAÇÃO** das **MEDIDAS** de segurança

g) **CONSEQUÊNCIAS** estimadas em caso não adoção de medidas adicionais

- Classificação de CONSEQUÊNCIAS – Exemplos

ALTAS

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

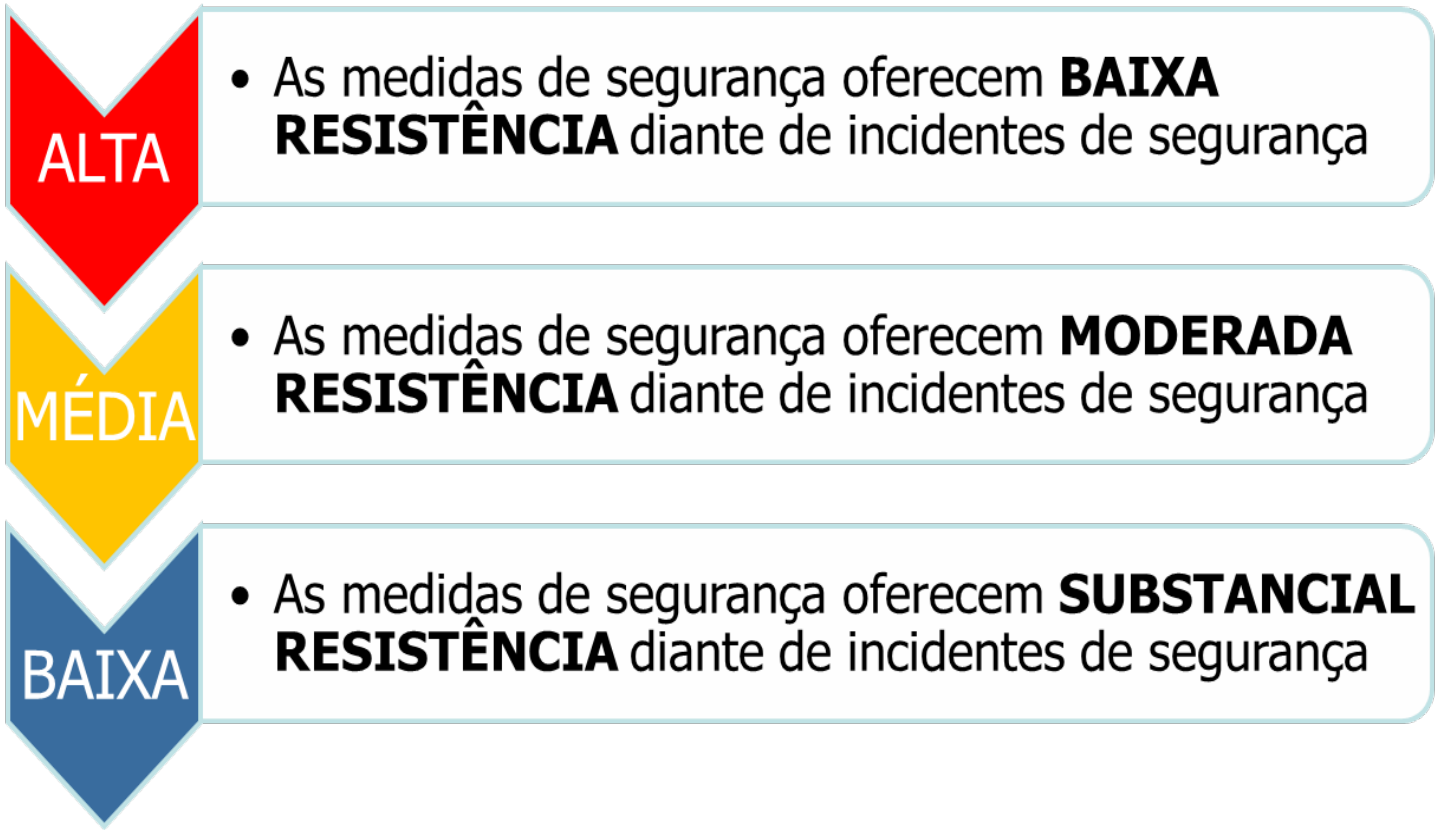
MÉDIAS

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

BAIXAS

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

- 3: Classificação da PROBABILIDADE de occorrerem INCIDENTES



- Classificação de INCIDENTES de SEGURANÇA.

CONSEQUÊNCIAS	PROBABILIDADE: ALTA	PROBABILIDADE: MÉDIA	PROBABILIDADE: BAIXA
ALTA	Contramedidas	Contramedidas	Avaliar
MÉDIA	Contramedidas	Contramedidas ou Avaliar	Documentar
BAIXA	Avaliar	Documentar	Documentar

- Definição de CONTRAMEDIDAS

Metodologia das normas ISO 28001 e ISO 20858

		CONSEQUÊNCIA		
		Alta	**Média**	**Baixa**
PROBABILIDADE	**Alta**	Contramedidas	Contramedidas	
	Média	Contramedidas		
	Baixa			

4.3.2 Requisitos legais e outros

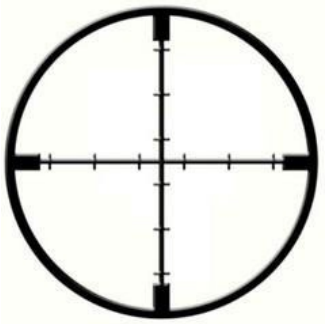
A organização deve estabelecer, implementar e manter um procedimento para:

- **Identificar e ter acesso** aos requisitos legais aplicáveis, e a outros requisitos estabelecidos pela própria organização relacionados com suas ameaças e riscos a segurança
- Determinar **como** estes requisitos **afetam** as ameaças e riscos a segurança
- **Manter e comunicar** os requisitos aos funcionários e terceiros, incluindo prestadores de serviço/fornecedores eventuais.

4.3.3 Objetivos da gestão de segurança

A organização deve estabelecer, implementar e manter **documentados** os **objetivos** de segurança, tendo em conta o seguinte:

- Os objetivos derivam da **política** e são coerentes com esta.
- Os **requisitos** legais, estatutários e outros requisitos regulamentares
- **Ameaças e riscos** relacionados a segurança
- As **opções** tecnológicas e de outro tipo
- Os **requisitos** financeiros, operacionais e comerciais
- **Visões** das partes interessadas
- Os objetivos devem ser coerentes com a **melhoria contínua**, quantificáveis, comunicados e revistos periodicamente.



4.3.4 Metas da gestão da segurança

A organização deve estabelecer, implementar e manter documentadas as **metas** de gestão de segurança, as quais:

- Devem estar **documentadas** e ser **apropriadas** à organização
- Devem decorrer dos objetivos e ser **coerentes** com eles.
- Devem ter um nível adequado de **detalhe**
- Devem ser específicas, **mensuráveis**, atingíveis, **relevantes** e estabelecidas no tempo
- Devem ser **comunicadas** e revistas periodicamente.

4.3.5 Programas de gestão da segurança

A organização deve estabelecer, implementar e manter **programas de gestão** de segurança, para alcançar seus objetivos e metas, tendo em conta o seguinte:

- Os programas devem ser **otimizados e priorizados**
- A organização deve proporcionar os meios para a implementação **eficiente** e **rentável**.
- Documentando:
  - As pessoas designadas, autoridade e **responsabilidade**
  - Os **meios** e o cronograma pelos quais os objetivos e metas devem ser alcançados.
- Devem ser revistos e, se necessário, modificados para assegurar que permaneçam eficazes e consistentes com os objetivos e metas.

4.4.1 Estrutura, autoridade e responsabilidade

As funções, responsabilidades e autoridade devem ser definidas, documentadas e comunicadas.

A gestão de topo deve evidenciar o seu **compromisso** com o desenvolvimento, a implementação do sistema de gestão de segurança (processos) e a melhoria contínua, mediante:

- A nomeação de um **membro da administração** como o responsável pela conceção, manutenção, documentação e melhoria do sistema de gestão de segurança .
- A nomeação os membros da administração com autoridade necessária para **assegurar** a implementação dos **objetivos e das metas**
- identificar e monitorizar os requisitos e expectativas das **partes interessadas** da organização
- A disponibilidade dos **recursos** necessários
- A **comunicação** à organização da importância de cumprir com os requisitos a fim de cumprir com a politica
- A garantia da **viabilidade** dos objetivos, metas e programas
- Considerar o impacto **adverso** que a politica (ou objetivos, metas, programas) possa ter sobre outros aspectos da organização.

4.4.2 Competência, formação e consciencialização

A organização deve assegurar que os **responsáveis** pela conceção, operação e gestão dos equipamentos e processos de segurança estejam adequadamente **qualificados** em termos de educação, formação e/ou experiência.

A organização deve manter **procedimentos** que assegurem que as pessoas que trabalham para ela ou em seu nome estejam conscientes:

- Da importância do **cumprimento** da política e dos procedimentos.
- Das suas funções e responsabilidades com a **conformidade**, incluindo resposta a emergências.
- Das **consequências** potenciais para a segurança em caso de desvio dos procedimentos operacionais especificados.

Os **registos** de competência e formação devem ser mantidos.

4.4.3 Comunicação

- Devem ser mantidos procedimentos que garantam que a informação pertinente de gestão da segurança seja comunicada aos **colaboradores, subcontratados e outras partes interessadas.**

- Devido à natureza sensível de determinadas informações relacionadas a segurança, deve-se considerar a **sensibilidade** dessas informações antes da sua divulgação.

4.4.4 Documentação

A organização deve estabelecer e manter um sistema de documentação da gestão de segurança que inclua:

- A política, os objetivos e as metas
- A descrição do **âmbito** do sistema de gestão da segurança
- A descrição dos elementos do sistema de gestão de segurança e, sua **interação** e a referência aos documentos relacionados
- Os documentos e **registos** requeridos pela norma e pela organização para assegurar o efetivo o planeamento, operação e controlo dos processos.
- Determinação do nível de **confidencialidade** ou sensibilidade da informação e tomar medidas para prevenir o acesso não autorizado.

4.4.5 Controle de documentos e dados

A organização deve estabelecer e manter **procedimentos** para controlar todos os documentos, dados e informação, assegurando que:

- Estão disponíveis e **acessíveis** somente para pessoas **autorizadas**
- Sejam revistos periodicamente e são aprovados pelas pessoas autorizadas
- As **versões atuais** dos documentos, dados e informações estejam disponíveis em todos os locais onde são realizadas as operações e que documentos obsoletos sejam retirados ou eliminados sem demora em todos os pontos, evitando o uso indevido
- Os documentos **retidos** para fins legais são adequadamente identificáveis.
- Garantir que todos os documentos estão seguros, mantendo cópias de segurança (documentos em formato eletrónico) que possam ser recuperadas.

4.4.6 controlo operacional

A organização deve identificar as **operações e atividades** que sejam necessárias para alcançar:

- A sua **política** de gestão da segurança
- O **controlo** das atividades e a **mitigação** das ameaças identificadas com risco significativo
- **Conformidade** com os requisitos legais e regulamentares
- Os **objetivos** da gestão da segurança
- A execução dos seus **programas** de gestão de segurança
- O nível requerido de **segurança** da cadeia de abastecimento.

Tudo isso mediante procedimentos documentados, para controlar situações onde sua ausência poderia levar a omissão na realização das operações

4.4.6 controlo operacional

Estes procedimentos devem incluir **controlos** para a conceção, instalação, operação, renovação e modificação de itens de equipamento, instrumentação, etc.

Quando as **disposições** existentes são revistas ou criadas novas disposições, antes da implementação, considerar as ameaças e riscos associados incluindo:

- A revisão da estrutura, funções e responsabilidade da organização
- A revisão de política, objetivos, metas e programas
- A revisão de processos e procedimentos
- A introdução de nova infraestrutura, como equipamentos ou tecnologia de segurança, que pode incluir hardware ou software
- A introdução de novos prestadores de serviço, fornecedores ou pessoal.

4.4.7 Prontidão, resposta a emergências e ...

A organização deve estabelecer, implementar e manter planos e procedimentos adequados para identificar os potenciais incidentes de segurança e situações de emergência.

Estes planos devem incluir:

- A resposta prevista para prevenir e mitigar as prováveis consequências
- A informação sobre o fornecimento e manutenção de qualquer equipamento, instalação ou serviço que possam ser exigidos durante ou apos incidentes ou situações de emergência

Os planos devem ser revistos periodicamente visando avaliar a sua eficácia, após ocorrências e testes, realizando para tanto te
periódicos (exercícios ou simulacros).

4.5.1 Monitoração e medição

A organização deve estabelecer e manter procedimentos para **monitorar** e medir o seu **desempenho,** proporcionando:

- **Medições** qualitativas e quantitativas
- Grau de **cumprimento** da política, objetivos e metas
- Medidas **proativas** de desempenho da conformidade com os programas, critérios de controlo operacional, legislação aplicável e outros requisitos
- Medidas **reativas** de desempenho para monitorar deterioração, falhas, incidentes, não conformidades, etc (inclusive quase ocorrências)
- registo de dados e resultados, suficiente para facilitar a análise de medidas preventivas e corretivas.
- registo das atividades de calibração e manutenção (ver 4.5.1.e)

4.5.2 Avaliação do sistema

- A organização deve **avaliar** os planos e procedimentos da gestão de segurança por meio de **análises periódicas**, relatórios pós incidentes, avaliações do desempenho, lições aprendidas, exercícios, etc...
- As **alterações** devem refletir-se de imediato nos procedimentos
- A organização deve avaliar periodicamente a **conformidade** com a legislação e regulamentos pertinentes, as melhores práticas industriais e a conformidade com sua própria política e objetivos
- A organização deve manter **registos** dos resultados dessas avaliações periódicas.

4.5.3 Falhas, incidentes, nC's e ACP's

Devem ser estabelecidos, implementados e mantidos procedimentos definindo **autoridade e responsabilidade** para:

- Avaliar e iniciar **ações preventivas**
- **Investigar** as falhas, quase ocorrências, incidentes e situações de emergência, não conformidades
- Tomada de ação para **mitigar** as consequências de falhas, incidentes e não conformidades
- Iniciar e fechar as ações corretivas
- Confirmar a eficácia das ações corretivas tomadas

As ações corretivas/preventivas devem ser **analisadas** por meio do processo de apreciação de riscos **antes da implementação**.

As ações propostas devem ser **apropriadas** à magnitude do problema e **proporcionais** às ameaças e riscos.

Rever procedimentos documentados e **treinar** pessoas.

4.5.4 controlo de registos

A organização deve manter **registos** que demonstrem a **conformidade** com os requisitos do seu sistema de gestão de segurança e da presente norma;

Um **procedimento** deve ser estabelecido para identificação, arquivo, proteção, recuperação, retenção e eliminação de registos;

Os registos devem ser e **permanecer** legíveis, identificáveis e rastreáveis;

A documentação eletrónica deve ter a sua **integridade** preservada, com cópia de segurança e ser acessível somente às pessoas autorizadas.

4.5.5 Auditoria

A organização deve estabelecer, implementar e manter um **programa de auditoria** de gestão da segurança, garantindo que as auditorias são realizadas a intervalos planeados, a fim de:

a) Determinar se o sistema de gestão de segurança:

   1) **Cumpre** com as ações previstas, incluindo os requisitos da secção 4 da presente norma

   2) Tem sido adequadamente **implementado** e **mantido**

   3) É **eficaz** no cumprimento da política e dos objetivos de gestão de segurança da organização.

b) Rever os **resultados** de auditorias anteriores e as **ações** tomadas para retificar as não conformidades;

c) Fornecer informações sobre os **resultados** das auditorias;

d) Verificar se os equipamentos e pessoal da segurança são adequadamente **empregues**.

4.6 Revisão pela gestão e melhoria contínua

A **gestão de topo** deve rever o sistema de gestão da segurança em intervalos planeados. Esta análise deve incluir a avaliação de **oportunidades** de melhoria e a necessidade de **mudanças**.

Elementos de entrada

- Resultados de **auditoria** interna/externa, inspeções, etc...
- **Comunicações** externas de partes interessadas, incluindo **reclamações**
- O **desempenho** da segurança
- O grau de **cumprimento** de objetivos e metas
- Estado das **ações** corretivas e preventivas
- Ações de **seguimento** de anteriores revisões pela gestão
- **Alterações** que possam afetar o sistema de gestão
- Recomendações de **melhoria**.

Os dados de saída devem incluir qualquer decisão ou ação relacionada com as possíveis mudanças na politica, objetivos, metas e outros elementos de maneira coerente com a melhoria contínua.

Contactos

- Rua da Bela Vista, n.º 110 – 2º A, Alcaniça,
- 2825-004 Caparica. Portugal.
- **Tel.:** (+351) 212 947 543

www.grupoqualiseg.com

support@grupoqualiseg.com

PROVIDING VALUE

ISO 9001: 2008 Certificate No: 50042

Direcção Geral de Energia e Geologia

Credenciação NATO Secret