QUALIseg
ENGENEERING AND MANAGEMENT

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

Sistema de Gestão da Segurança da Informação (SGSI)

Projecto:

GISAMP

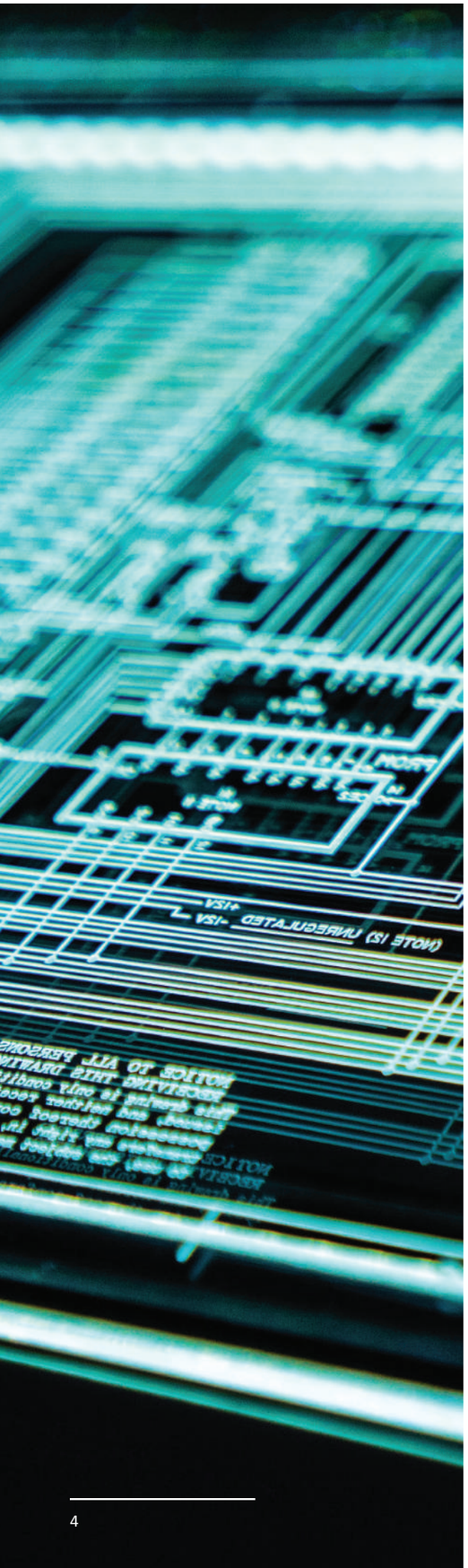
Cofinanciado por:

REPÚBLICA PORTUGUESA
MAR

fundoazul

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

Índice



1

Introdução à norma ISO 27001

Todas as organizações têm acesso e/ou possuem informação valiosa ou sensível. Em caso de falhas na proteção dessa mesma informação pode levar a danos incalculáveis a nível das operações, perdas financeiras ou mesmo consequências legais severas. Em casos extremos, essas falhas podem mesmo levar ao encerramento da organização.

O maior desafio apresentado às organizações neste aspeto é como providenciar proteção adequada a essa informação. Particularmente, como deverão garantir que identificaram todos os riscos a que estão expostos, bem como geri-los de uma forma sustentável, proporcional e eficiente a nível de custo.

A ISO 27001 é a norma internacional reconhecida para o Sistema de Gestão da Segurança da Informação. Apresenta métodos e requisitos para garantir a proteção da informação que podem ser adaptados a todos os sectores e dimensões das organizações. Nos últimos anos, organizações com uma exposição significativa aos riscos relacionados com a segurança da informação tem escolhido implementar sistemas de gestão em conformidade com este referencial.

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

A Família 27000

A série de normas 27000 começou em 1995 com a BS 7799, escrita na altura pelo Department of Trade and Industry (DTI) do Reino Unido. As normas da família 27000 têm o prefixo "ISO/IEC" devido a terem sido desenvolvidas e mantidas em conjunto por duas organizações normativas: ISO (International Organization for Standardization) e o IEC (International Electrotechnical Commission). Porém, de forma a simplificar a sua apresentação, geralmente só o prefixo "ISO" é utilizado.

Existem atualmente 45 normas publicadas na família 27000. De todas elas, somente a ISO 27001 é certificável. As restantes são elementos guia e de implementação de boas práticas na segurança da informação.

Atualizações e revisões regulares

As normas ISO são sujeitas a revisão a cada cinco anos de forma a validar se é necessário a sua atualização. A última revisão à norma ISO 27001 foi em 2013 e trouxe uma mudança significativa através da adoção da estrutura do Anexo SL.

Três das normas da família 27000 são particularmente consideradas um bom auxílio na implementação do Sistema de Gestão da Segurança da Informação:

- ISO 27000 - *Information Technology – Overview and vocabulary* – Terminologia da família 27000;
- ISO 27002 - *Information Technology – Security Techniques* – Código de boas práticaspara a implementação dos Controlos para a Segurança da Informação. Estes controlos estão descritos no Anexo A da ISO 27001;
- ISO 27005 – *Information Technology – Security Techniques – Information Security Management* – Gestão de Risco a nível de Segurança da Informação

2

Benefícios da **implementação** da **norma ISO 27001**

A Segurança da Informação é um fator de extrema importância para as organizações e a implementação de um referencial como a ISO 27001 é cada vez mais vista como uma necessidade. A maior parte das organizações já chegaram à conclusão que a pergunta a fazer não é se serão afetadas por uma falha de segurança, mas sim, quando serão afetadas.

A implementação de um Sistema de Gestão de Segurança da Informação e a sua certificação segundo a ISO 27001, quando realizada de forma eficaz e eficiente, traz vários benefícios, geralmente divididos em 3 áreas:

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 adoção da ISO 27001, bem como clientes já certificados têm como tendência trabalhar com fornecedores com a mesma certificação, tendo assim garantias que os seus dados e processos são mantidos seguros.

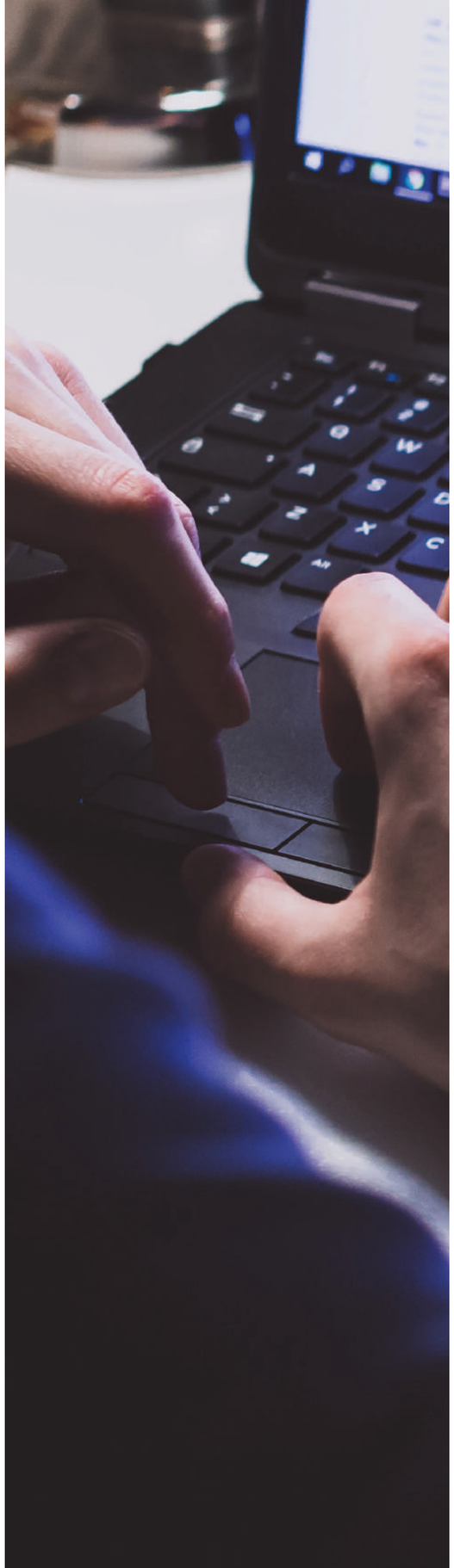
Garantia de Segurança

Muitas organizações possuem ou têm acesso a informação que é crítica no desenrolar das suas operações, vital para o desenvolvimento do seu negócio ou que é parte fundamental na sua saúde financeira.

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 27001 é a norma internacionalmente reconhecida para a implementação de um Sistema de Gestão da Segurança da Informação, garantindo com a sua certificação a validação por uma equipa independente.

Operações

Com a sua abordagem holística, a ISO 27001 dá suporte ao desenvolvimento de uma cultura interna na organização onde a perceção 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**

O principal propósito do Sistema de Gestão da Segurança da Informação é garantir a proteção da informação sensível ou valiosa.

Informação sensível geralmente inclui informação sobre colaboradores, clientes e fornecedores. Informação valiosa pode incluir propriedade intelectual, dados financeiros, dados legais, informação comercial e dados de operação.

Podemos agrupar os principais tipos de risco a que a informação sensível ou valiosa está sujeita em 3 categorias:

- Confidencialidade: quando uma ou mais pessoas têm acesso indevido a informação.
- Integridade: quando o conteúdo da informação é alterado, tornando essa informação incompleta ou não confiável.
- Disponibilidade: quando o acesso à informação é perdido ou tornado difícil.

3 Principais conceitos e terminologia

Esta tipologia de risco é conhecida como “CIA” (Confidentiality, Integrity and Availability).

O Risco em Segurança da Informação é medido quando uma ameaça explora uma determinada vulnerabilidade de um ativo de informação, levando assim a incidentes.

Ativos de Informação neste contexto podem ser colaboradores, equipamentos, sistemas ou infraestrutura.

Informação é o conjunto de dados que uma organização que proteger, tais como dados de colaboradores, dados de cliente e/ou fornecedor, dados de acesso, dados financeiros, etc.

Incidentes são eventos nefastos que resulta na perda de confidencialidade (acesso indevido), integridade (dados alterados) e/ou disponibilidade (perda de acesso à informação) de determinada informação

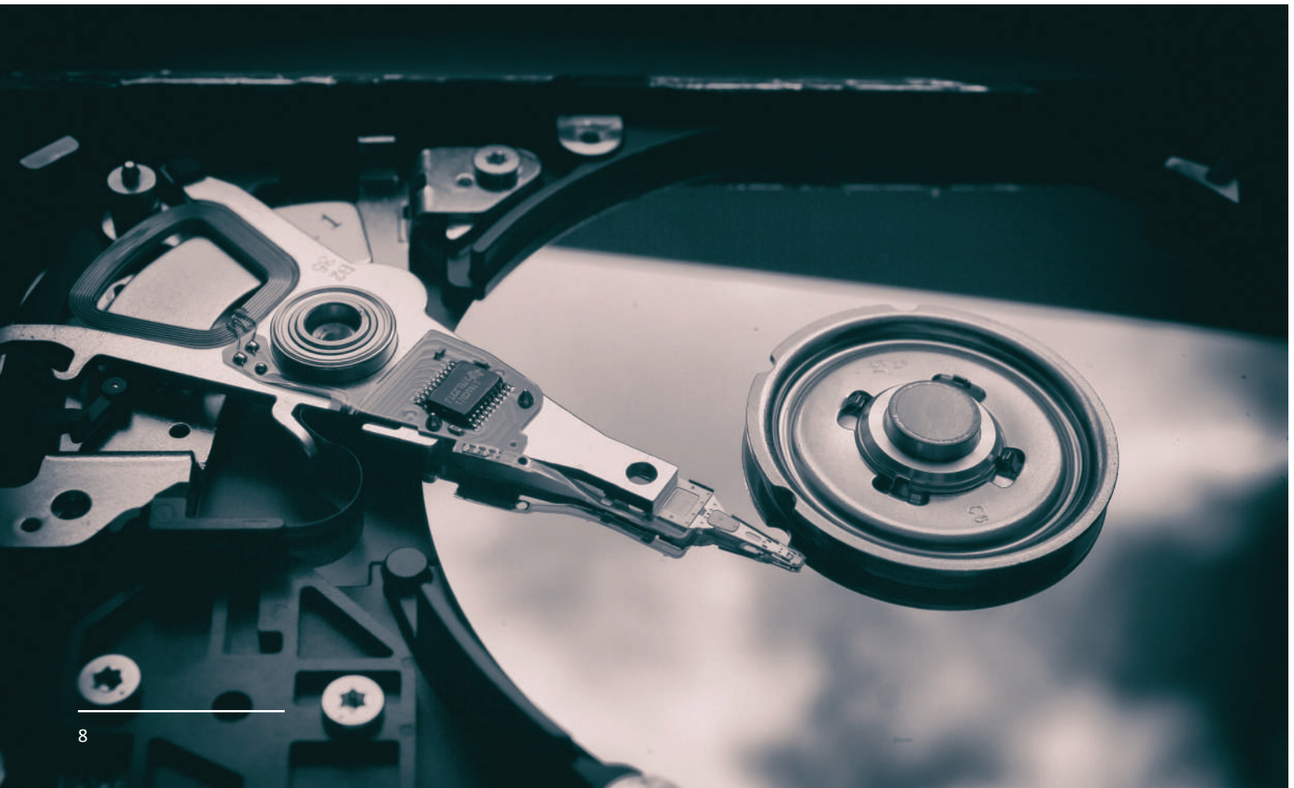
Ameaças são a causa dos incidentes e podem ser maliciosas (um assalto), acidentais (erro na inserção de dados) ou fortuitas (cheia).

Vulnerabilidades tais como erros de desenvolvimento, fraca proteção a nível de acesso físico, proximidade a perigos naturais vão potenciar que a presença de uma ameaça as explore, levando assim ao incidente.

Um risco de segurança de informação é gerido através de um sistema de gestão devidamente implementado e dos seus controlos de segurança, tais como proteção contra incêndios, acesso restrito ou backups de informação.

Um sistema de gestão implementado de acordo com a ISO 27001 terá uma abordagem de processos que facilitará a implementação, revisão e manutenção desses mesmos controlos, garantindo assim a mitigação dos riscos associados à informação.

.



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:

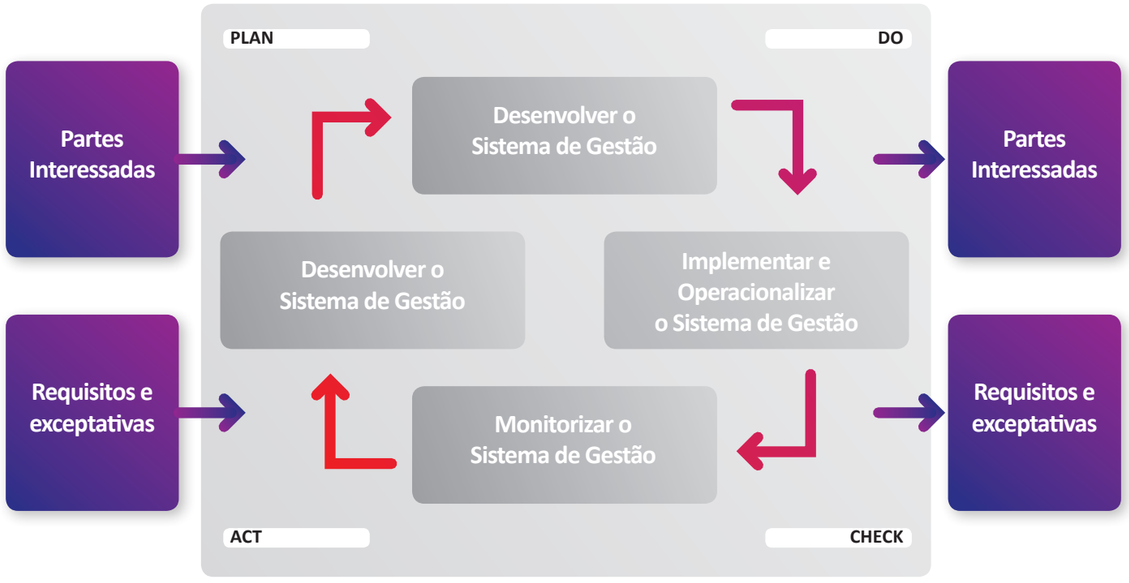
1. Plan (Planeamento)
Estabelecer objectivos, recursos necessários, requisitos das partes interessadas, políticas organizacionais e identificar risco e oportunidades.

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.

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.

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.

7 Gestão Integrada

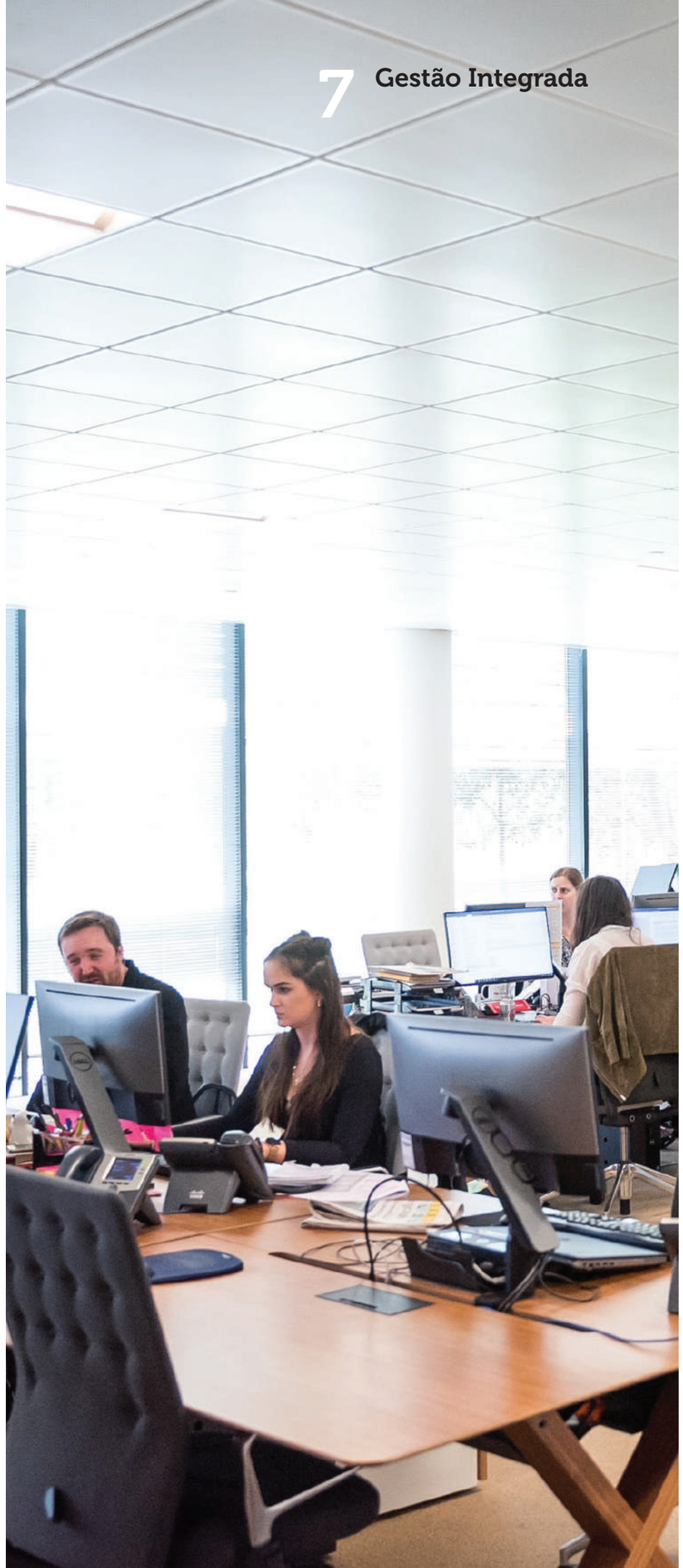
O desenvolvimento de um Sistema Integrado de Gestão deverá ser suportado por conceitos devidamente pensados e coerentes. Este Sistema tem associado:

- 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.

O desenvolvimento de um Sistema Integrado de Gestão deverá ser suportado por conceitos devidamente pensados e coerentes



7 Gestão Integrada

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

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 cláusulas:

- 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 27001

A ISO 27001 é composta por 10 secções conhecidas como Cláusulas.

Tal como a maior parte das normas relativas a Sistemas de Gestão, os requisitos da norma estão entre as cláusulas 4.0 a 10.0. Mas, ao contrário da maioria das normas relativas a Sistemas de Gestão, a ISO 27001 exige que exista cumprimento com todos os requisitos da norma, não sendo possível declarar a não-aplicabilidade de algum.

Na ISO 27001, em adição às cláusulas 4 a 10, existe também o **Anexo A** (que é referido na cláusula 6). O Anexo A contêm 114 controlos: boas práticas que apoiam na proteção da informação. Cada um destes controlos deve ser considerado por parte da organização e, caso algum não seja aplicável, deverá ser apresentada uma justificação para a sua não-implementação.

As próximas secções deste manual apresentam cada Cláusula da ISO 27001, bem como sugestões de implementação de cada requisito.

Requisitos Gerais

A Cláusula 1 da ISO 27001 apresenta:

- o objetivo da norma;
- a tipologia de organizações a que a norma se destina;
- as secções da norma (chamadas Cláusulas) que contêm requisitos com os quais uma organização deverá cumprir no seu Sistema de Gestão.A ISO 27001 é destinada a todo o tipo de organização, independentemente do sector, dimensão, maturidade ou complexidade.

Contexto da Organização

O propósito do Sistema de Gestão é proteger os ativos de informação da organização, de modo a que a organização consiga atingir os seus objetivos.

O contexto da organização pode ser dividido em duas áreas:

- Contexto interno: áreas onde a organização tem controlo;
- Contexto externo: áreas onde a organização não tem controlo direto e pode apenas influenciar indiretamente.

Contexto Interno

A organização deverá avaliar os seus aspetos internos que possam ter influência direta nos riscos do seu sistema de gestão, tais como:

- Maturidade da Organização
- Cultura Organizacional
- Gestão
- Disponibilidade de recursos
- Maturidade dos recursos
- Formatos principais dos ativos de informação
- Valor e sensibilidade dos ativos de informação
- Consistência dos processos
- Sistemas e a sua complexidade
- Espaço e ambiente físico

Contexto externo

Tal como relativamente aos aspetos internos, os aspetos externos também deverão ser avaliados sobre o impacto que possam ter nos riscos do sistema de gestão, tais como:

- Concorrência
- Espaço e ambiente externos
- Legisladores e regulamentadores
- Perspetiva económica e política
- Considerações a nível do Meio Ambiente
- Prevalência de ataques informáticos no sector/área de atividade ou região
- Partes Interessadas

Partes Interessadas

Uma parte interessada é todo o elemento que é, pode ser, ou tem a perceção de ser afetado pelas ações (ou inações) da organização. Durante a análise do contexto interno e externo, a composição das partes interessadas ficará mais clara. Exemplos diretos de partes interessadas são os colaboradores da organização, clientes, fornecedores, comunidade envolvente e Estado.

Deverão ser levantados os requisitos das partes interessadas relevantes para o Sistema de Gestão, bem como avaliar o cumprimento dos mesmos.

Âmbito do Sistema de Gestão

Para cumprir com os requisitos da ISO 27001, a organização deverá documentar o âmbito do seus sistema de Gestão. Na generalidade, o âmbito documentado deverá descrever:

- As fronteiras da localização (ou localizações) física
- As fronteiras das redes físicas e lógicas incluídas
- Os grupos de colaboradores (internos e externos) incluídos ou excluídos
- Os serviços e processos internos incluídos
- Interfaces essenciais nas fronteiras do âmbito.

Uma forma de priorizar recursos é implementar um Sistema de Gestão com um âmbito mais reduzido, sendo que esse sistema não irá abranger a totalidade da organização ou serviços.

8 Cláusulas normativas da ISO 27001

Liderança

Liderança no contexto da ISO 27001 significa envolvimento cativo no desenho do Sistema de Gestão, bem como providenciar os recursos necessários e apoiar a implementação. Estes pontos incluem a garantia de que:

- Os objetivos do Sistema de Gestão são claros e alinhados com a estratégia geral
- As responsabilidades são definidas e estruturadas
- O pensamento baseado no risco é assegurado ao longo de todas as decisões
- A comunicação é feita de forma eficiente e transversal a todas as partes interessadas no âmbito do Sistema de Gestão.

Política de Segurança da Informação

Uma das responsabilidades da Liderança é a criação e garantia de disponibilização da Política de Segurança da Informação, que deve estar alinhada com os objetivos estratégicos da organização, bem como devidamente documentada.

Deverá fazer referência ou conter diretamente:

- Os objetivos de segurança da informação, ou proporcionar um modelo de referência para a definição dos mesmos;
- O compromisso para satisfazer os requisitos aplicáveis que são relacionados com a segurança da informação;
- O compromisso para a melhoria contínua do Sistema de Gestão.

Funções, Autoridades e Responsabilidades

A gestão de topo deve garantir que as funções, autoridades e responsabilidades a nível do Sistema de Gestão se encontram definidas, entendidas e comunicadas. Deve também atribuir as mesmas para:

- Assegurar que o Sistema de Gestão se encontra em conformidade com os requisitos desta norma;
- Reportar à gestão de topo o desempenho do Sistema de Gestão.

Planeamento

A ISO 27001 pode ser encarada como uma ferramenta de gestão de risco, que aponta a organização para a identificação de riscos de segurança em todas as suas fontes. Como tal, o seu principal propósito é:

- Identificar os riscos estratégicos, importantes, diretos e escondidos na organização;
- Garantir que as atividades e operações da organização são desenvolvidas, dirigidas e com os recursos necessários para gerir esses riscos;
- Desenvolver respostas imediatas e automatizadas para lidar com novos riscos, minimizando continuamente o seu impacto na organização.

A gestão de topo deve garantir que as funções, autoridades e responsabilidades a nível do Sistema de Gestão se encontram definidas, entendidas e comunicadas.

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

8 Cláusulas normativas da ISO 27001

Avaliação do Risco

Para todas as organizações, a avaliação do risco é essencial para:

- Aumentar a possibilidade de identificar todos os riscos potenciais, através do envolvimento de colaboradores chave e uma metodologia de avaliação sistemática;
- Alocar os recursos adequados para as áreas críticas;
- Dar apoio às decisões estratégicas de como gerir os riscos de segurança de informação .

A organização deverá definir e aplicar um processo de avaliação de risco, sistemático e metódico, que estabeleça e mantenha critérios do risco, incluindo:

- Os critérios para a aceitação do risco;
- Os critérios para a realização de avaliações de risco;

Esse processo deverá também:

- Identificar os riscos de segurança da informação associados com a perda de confidencialidade, disponibilidade e integridade, bem como os responsáveis pelos mesmos;
- Analisar os riscos, avaliando as suas consequências caso aconteçam, probabilidade e níveis de risco;
- Avaliar os riscos, comparando o resultado dessa avaliação com os critérios estabelecidos;
- Estabelecer prioridades para o tratamento dos riscos analisados.

Tratamento do Risco

Para cada risco avaliado, deverá ser tomada uma decisão baseada em critérios claros e repetíveis de:

- Aceitar o Risco
- Tratar o Risco

Esse plano de tratamento do risco, que conterá as ações para tratar os riscos, salvo em situações onde o risco for aceite, deverá ser devidamente documentado.
O plano de tratamento do risco geralmente contêm opções de:

- Evitar o risco – parar de realizar a atividade ou o processamento dessa informação
- Remover o risco – eliminar a causa do risco
- Alterar a Probabilidade – implementar um controlo que irá alterar a probabilidade de um incidente de segurança da informação acontecer
- Alterar a Consequência – implementar um controlo que diminuirá o impacto caso ocorra um incidente de segurança

Anexo A e Declaração de Aplicabilidade

Todas as opções para o tratamento do risco – com exceção da aceitação do risco – envolvem a implementação dos controlos do Anexo A da norma ISO 27001. O Anexo A contêm 114 controlos de boas-práticas para a implementação de segurança da informação.
Aquando da preparação do Plano de Tratamento do Risco, a organização deverá escolher a aplicação dos controlos necessários. A ISO 27002 contêm mais informação para a aplicação de cada controlo presente no Anexo A.

A organização deve documentar também a sua Declaração de Aplicabilidade. Nesta declaração, deverá indicar para cada um dos 114 controlos:

- A sua aplicabilidade no Sistema de Gestão da Organização;
- Se foram aplicados ou não;
- Caso não sejam aplicáveis, deverá ser indicada a razão para a sua não aplicação.

Objetivos de Segurança da Informação

A organização deverá definir objetivos de Segurança da Informação que:

- Sejam mensuráveis;
- Estejam alinhados com a Política de Segurança da Informação;
- Tenham em consideração o resultado da Avaliação e Tratamento do Risco.

Deverão também considerar:

- O que será feito;
- Os recursos necessários;
- Quem será responsável;
- Quando estará concluído;
- Como os resultados serão avaliados.

8 Cláusulas normativas da ISO 27001

Suporte

A cláusula 7 diz respeito à alocação de recursos, sejam eles recursos humanos, infraestrutura, outros recursos físicos bem como o conhecimento na organização. Quando se realiza o planeamento dos objetivos do Sistema de Gestão, a Capacidade e Adequação dos recursos internos e externos deverá ser um ponto chave nas decisões estratégicas da organização.

Competência

A implementação de controlos de segurança da informação de uma forma eficaz depende profundamente do conhecimento e competências dos recursos humanos da organização, bem como dos seus fornecedores críticos. De forma a garantir que os mesmos são apropriados, a organização deverá:

- Definir que conhecimento e competências são necessárias;
- Determinar quem necessita desse conhecimento;
- Garantir que, quando necessário, empreende as ações para atingir os desejados níveis, através de formação ou outras, assegurando também a eficácia da mesma.

Consciencialização

Para além da garantia das competências dos recursos críticos a nível de segurança da informação, a organização deverá garantir também a consciencialização da restante organização e fornecedores críticos para o tema da Segurança da Informação e especialmente para o Sistema de Gestão. Para tal, toda a organização, fornecedores ou sub-contratados deverão estar conscientes que:

- A organização tem um Sistema de Gestão e quais são as razões para o ter;
- Existe uma Política de Segurança da Informação e quais os pontos-chave;
- Como podem contribuir para a segurança da informação da organização, bem como o atingir dos seus objetivos;
- Quais são as políticas, procedimentos e controlos que são relevantes para eles e quais são as consequências do seu incumprimento.

Comunicação

De forma a garantir o funcionamento correto dos processos do Sistema de Gestão, as atividades de comunicação deverão ser planeadas e geridas. O requisito de comunicação da ISO 27001 aponta para que a organização defina:

- A frequência da comunicação;
- Os destinatários;
- Quem é responsável pela comunicação;
- Quais são as formas e/ou processos para a comunicação.

Informação Documentada

A informação documentada que é utilizada para implementar e manter o Sistema de Gestão deve:

- Ser precisa e clara;
- Ser compreensível por parte dos recursos humanos que a utilizam regularmente ou ocasionalmente;
- Ser adequada à dimensão e complexidade do sistema de gestão e da organização;
- Ser revista atempadamente
- Ser controlada relativamente à sua disponibilização, acesso, identificação e controlo de versões;

A informação deverá ser documentada conforme requerida pelos controlos implementados.

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

8 Cláusulas normativas da ISO 27001

Operações

Após a fase de planeamento e de avaliação do risco, entramos na fase de operação. A cláusula 8 tem o objetivo de garantir que a organização tem o nível de controlo apropriado na entrega do produto ou serviço.

Gerir os riscos de segurança da informação e atingir os objetivos requer a formalização das atividades num conjunto de processos coerentes.

Habitualmente, muitos desses processos já estão definidos (exemplo: processo de formação e recrutamento), requerendo assim apenas a sua adaptação e normalização de forma a incluírem elementos relevantes para a segurança da informação. Outros processos terão agora de ser definidos (exemplo: auditoria interna).

De forma a obter uma correta definição dos processos, os seguintes passos são cruciais:

- Os processos são criados por adaptação e/ou formalização das atividades habituais da organização.
- Identificação sistemática dos riscos de segurança da informação relevantes a cada processo;
- Definição clara e comunicação das atividades necessárias para gerir os riscos de segurança de informação decorrentes de um determinado evento (exemplo: entrada de um novo colaborador)
- Definição clara das responsabilidades de cada atividade;
- Alocação de recursos necessários;
- Avaliação periódica da consistência de cada processo e da sua eficiência em gerir os riscos de segurança da informação relevantes.

Avaliação de Risco

A metodologia e as técnicas de avaliação de risco definidas na cláusula 6 deverão ser aplicadas a todos os processos, cativos, informação e atividades dentro do âmbito do Sistema de Gestão.

Como os riscos não são estáticos, os resultados da avaliação de risco deverão ser revistos periodicamente (pelo menos uma vez ao ano), quando surge alguma alteração ou no caso da persistência de riscos elevados. Os riscos deverão ser revistos quando:

- As ações de Tratamento do Risco são finalizadas;
- Existem alterações significativas aos cativos, informação ou processos;
- Novos riscos são identificados;
- Experiência ou nova informação indica que as consequências de qualquer risco identificado possam vir a alterar.

Tratamento do Risco de Segurança da Informação

O plano de tratamento de risco necessita de ser implementado de acordo com o planeado. O impacto do plano deverá também de ser avaliado, bem como os resultados do mesmo deverão ser registados.

Estes pontos poderão ser executados durante a Revisão pela Gestão ou a Auditoria Interna, ou com a utilização de outras ferramentas técnicas, tais como testes de intrusão, auditorias de 3ª parte ou auditorias a fornecedores.

8 Cláusulas normativas da ISO 27001

Avaliação do Desempenho

Existem três principais formas de avaliar o desempenho do Sistema de Gestão:

- Monitorização da eficácia dos controlos do Sistema de Gestão;
- Auditorias Internas;
- Revisão pela Gestão.

O plano de tratamento de risco necessita de ser implementado de acordo com o planeado. O impacto do plano deverá também de ser avaliado, bem como os resultados do mesmo deverão ser registados.

Monitorização, Medição, Análise e Avaliação

A organização necessita decidir o que monitorizar de forma a assegurar que os processos e os controlos de segurança da informação estão a funcionar como previsto e são eficazes no Sistema de Gestão. Como não é exequível monitorizar todos os pontos a toda a hora, esta decisão necessita de ser tomada. Para tal, as considerações seguintes são importantes:

- Que processos e atividades estão sujeitos a ameaças mais frequentes e significativas?
- Que processos e atividades possuem as vulnerabilidades mais significativas?
- O que é prático de monitorizar e que gera dados significativos para a organização?

Para cada processo de monitorização que é estabelecido, deverá ser definido:

- Como e quando a monitorização é feita;
- Quem são os responsáveis;
- Como os resultados são apresentados e reportados, a quem e que análise é feita;
- Caso os resultados identifiquem um desvio do esperado, como se deve escalar a situação.

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

8 Cláusulas normativas da ISO 27001

Revisão pela Gestão

A revisão pela gestão é um elemento essencial de um Sistema de Gestão. É a formalização do ponto onde a gestão de topo revê a eficácia do Sistema de Gestão, bem como o seu alinhamento à orientação estratégica da organização.

A Revisão pela Gestão deverá ser realizada em intervalos programados e deverá analisar e documentar os resultados das seguintes áreas:

- Estado das ações resultantes de revisões anteriores;
- Alterações em questões internas e/ou externas relevantes para o Sistema de Gestão;
- **Informação recebida sobre o desempenho do Sistema de Gestão, nomeadamente:**
  - não conformidades e ações corretivas;
  - resultados das monitorizações e medições;
  - resultados das auditorias;
  - cumprimento dos objetivos do Sistema de Gestão.
- Informação das partes interessadas;
- Resultados da avaliação do risco e do plano de tratamento do risco;
- Oportunidades para a melhoria contínua.

Como saídas da Revisão, deverão ser consideradas:

- Decisões relativas a oportunidades de melhoria contínua;
- Qualquer necessidade de alterações ao Sistema de Gestão.

Auditorias Internas

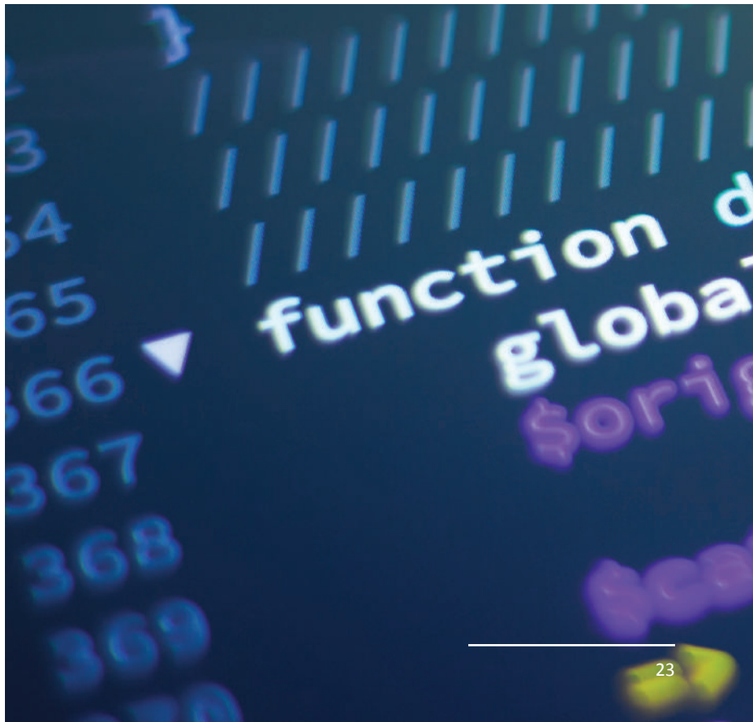
O principal propósito das Auditorias Internas é o teste aos processos do Sistema de Gestão, de modo a identificar os seus pontos fracos, bem como levantar oportunidades de melhoria. Ao mesmo tempo, as Auditorias Internas servem para validar a implementação e a coesão do Sistema de Gestão, vulgo, testar a sua performance.

- As Auditorias Internas deverão verificar:
- A consistência dos processos, procedimentos e controlos, a nível da sua aplicação;
- Se os resultados dos processos, procedimentos e controlos são os esperados;
- Se o Sistema de Gestão se mantêm alinhado e respeita os requisitos da ISO 27001, bem como outros requisitos de partes interessadas.

De forma a garantir que as auditorias são levadas a cabo de forma eficaz, bem como garantem a verificação dos pontos descritos em cima, elas deverão ser executadas por indivíduos que:

- Garantem a competência necessária;
- São independentes dos processos a auditar.

A organização deverá ter um programa de base periódica (geralmente anual) onde planeie as auditorias ao Sistema de Gestão.



8 Cláusulas normativas da ISO 27001

Melhoria

O foco da implementação do Sistema de Gestão deverá ser a redução da probabilidade de acontecimento de eventos nefastos de segurança da informação e a redução do seu impacto. Contudo, um Sistema de Gestão bem implementado e revisto irá melhorar ao longo do tempo e garantir o aumento de resiliência da organização face a ataques de segurança da informação.

Um dos pontos chaves da Melhoria é reter as lições aprendidas nos acidentes de segurança, nas constatações de auditoria, falhas de desempenho identificadas na monitorização, reclamações das partes interessadas e ideias e sugestões geradas nas revisões.

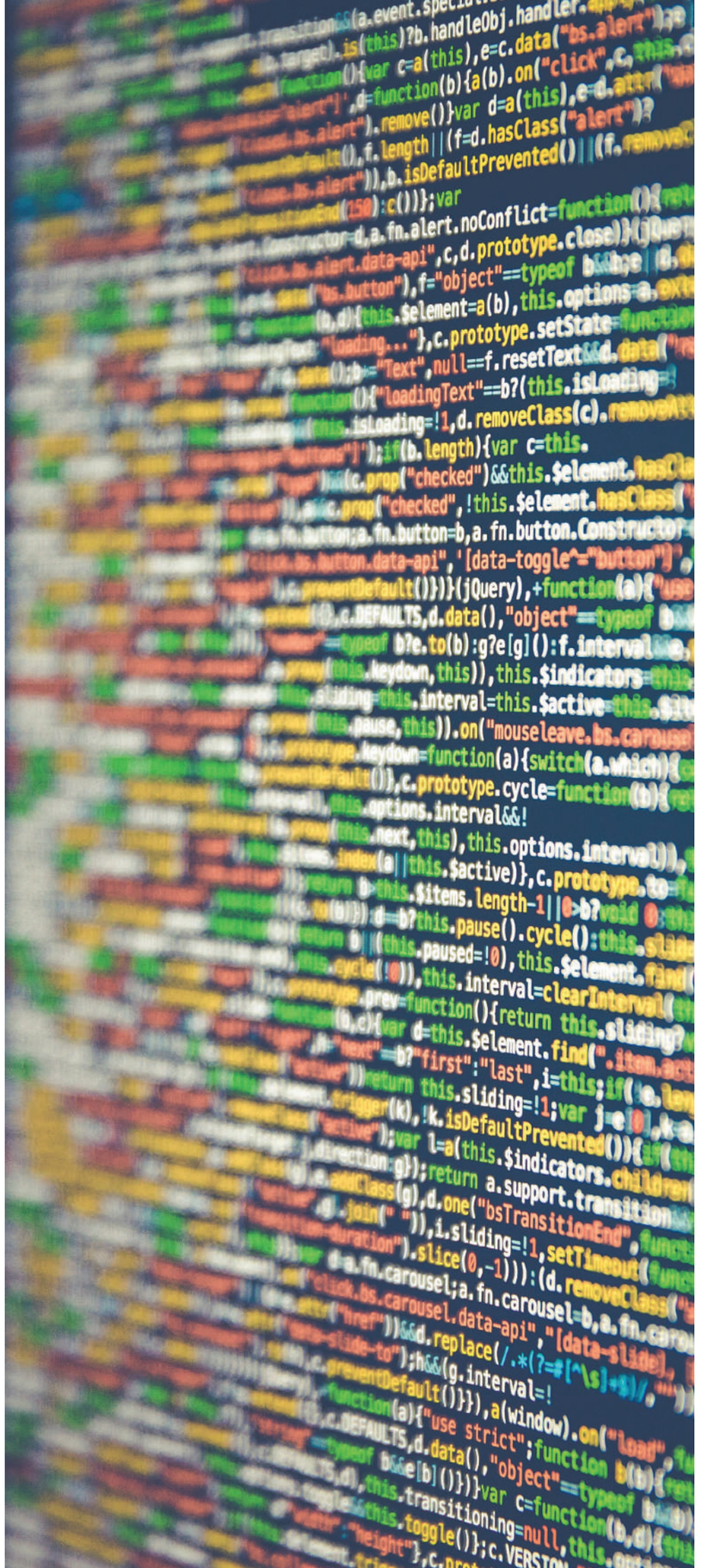
Para cada constatação identificada, a organização deverá manter um registo de:

- O que ocorreu;
- Caso tenha tido consequências indesejáveis, que ações foram tomadas para conter, corrigir ou mitigar a ameaça;
- Qual a sua causa raiz;
- Qual a ações que foram tomadas para eliminar a causa raiz;
- Qual a eficácia dessas ações.

Análise de Causas

Para garantir a implementação eficaz de uma ação corretiva, a mesma deverá ser focalizada na eliminação da causa raiz do acontecimento indesejável. Se a causa não for tratada convenientemente, a probabilidade de repetição desse evento será grande – se aconteceu uma vez, pode acontecer mais.

As causas raiz de um acontecimento nefasto deverão ser identificadas corretamente. Para tal, existem várias metodologias, uma das mais comuns é a do "5 Porquês", que consiste em perguntar o "porquê" do acontecimento cinco vezes até chegarmos a uma única causa, identificando assim a raiz do acontecimento. Para situações mais complexas, "5 Porquês" poderão não ser suficientes, sendo necessário aumentar o número de perguntas até chegar a uma única causa.



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).

Manual de Boas Práticas desenvolvido com base na norma ISO 27001:2013

10
Referências

1. *ISO 27001 - Information technology - Security techniques - Information security management systems - Requirements*
2. *ISO 27000 - Information Technology – Overview and vocabulary* – Terminologia da família 27000;
3. *ISO 27002 - Information Technology – Security Techniques* – Código de boas práticas para a implementação dos Controlos para a Segurança da Informação. Estes controlos estão descritos no Anexo A da ISO 27001;
4. *ISO 27005 – Information Technology – Security Techniques – Information Security Managemen*t – Gestão de Risco a nível de Segurança da Informação
5. *ISO 9001 - Quality management systems — Requirements;*
6. *ISO 31000 – Risk Management – Principles and Guidelines;*
7. *ISO Guide 73, Risk management — Vocabulary;*

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