Silvana Ponce

PANORAMA GERAL

ISO 27001:2013
ISO 27701:2020

Sistema de Gestão da Segurança e Informação
Sistema de Gestão de Informação Privada

QMS
Certification
Services

A QMS é um organismo de certificação de origem Australiana com atuação global, atualmente presente em mais de 30 países atuando especificamente com foco em certificação de sistemas de gestão e treinamentos de normas aplicáveis. A atuação da QMS na América é gerenciada por escritórios no Brasil e Estados Unidos da América com crescimento constante no continente em número de certificações e reconhecimento de mercado pelo nível técnico, satisfação de seus clientes e atendimento diferenciado.

A QMS é uma organização norteada por sua missão de **CONSTRUIR UMA SOCIEDADE MAIS FORTE ATRAVÉS DAS CERTIFICAÇÕES**, de seus valores sólidos e de seu código de conduta, assim a QMS acredita que pode transformar, fazer diferente e ser um organismo de certificação diferente.

SUMÁRIO

Introdução

Para proteção do dado pessoal é necessário a Segurança da Informação?

Vivemos em uma era tecnológica, em que a maior parte das informações está armazenada em dispositivos eletrônicos e o risco de acesso indevido ou vazamento de informações aumenta significativamente. O crescente número de vazamentos de informações de usuários nos diversos sites e serviços de armazenamento deixa claro a importância da implementação de controles de segurança da informação. A segurança da informação é entendida como um conjunto de ações para a proteção de dados de pessoas físicas e jurídicas.

Outro fator que também impulsionou a procura por controles de segurança da informação, foi o surgimento e necessidade de adequação à nova Lei Geral de Proteção de Dados (LGPD). De acordo com o Art. 46. da Lei 13709, “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais e sensíveis de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”, (CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS - Seção I - Da Segurança e do Sigilo de Dados), Na busca por adequação à LGPD e boas práticas de segurança da informação muitas empresas estão descobrindo a ISO 27701 e a ISO 27001.

ISO 27001 VS ISO 27701

A norma ISO 27001 – Sistema de Gestão de Segurança da Informação é uma norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão em segurança da informação, enquanto a norma ISO 27701 – Sistema de Gestão da Privacidade da Informação é uma extensão da norma ISO 27001 e ISO 27002 - Código de prática para controles de segurança da informação, tem como objetivo adicionar novos controles ao sistema de gestão da informação para auxiliar as empresas na gestão de riscos de privacidade relacionados com dado pessoal.

Vale ressaltar que é necessário implementar a ISO 27001 para que possa atender também a ISO 27701, porém não é possível implementar somente a ISO 27701 sem a ISO 27001, pois os controles relacionados a um sistema de gestão de segurança da informação estão na ISO 27001. As duas normas podem ser implementadas simultaneamente como um único sistema de gestão.

Por que é importante a segurança da informação?

A importância da segurança da informação é extrema, independentemente do tamanho organização ou ramo de atuação, é fundamental tratar as informações como os maiores bens da organização e nunca foi tão importante protegê-los, como no cenário atual. Qualquer dano a elas pode custar todo o futuro de uma organização, afetando a imagem, os negócios e planejamentos futuros.

Não é exagero dizer que um ataque cibernético bem sucedido representaria uma perda incalculável. Ao negligenciar a segurança da informação, não coloca apenas a organização em risco, mas também os dados e informações de clientes e parceiros comerciais.

Desafios

Existem diversas ameaças que colocam em risco os dados e arquivos de uma empresa, as principais ameaças sofridas pelas empresas são:

• INFECÇÃO POR MALWARE

A infecção por malware se dá por qualquer software ou parte de um software que tenha sido escrito ou reescrito com código malicioso causando danos aos dados e dispositivos da empresa.

• EXPLORAÇÃO DE VULNERABILIDADES

Esse tipo de ameaça ocorre quando hackers buscam falhas de segurança decorrentes da negligência das empresas. Os fatores de risco podem ser diversos, entre eles: falta de controles e atualizações, configurações mal feitas, redes desprotegidas, softwares com falhas e falta de treinamento dos funcionários.

• PHISHING

É um ataque por meio de fraude eletrônica com o objetivo de adquirir dados pessoais ao se fazer passar por uma pessoa ou empresa de confiança, uma “comunicação eletrônica oficial” é enviada através de e-mail, mensagem instantânea ou SMS.

• ACESSO INDEVIDO

O acesso indevido viola um dos princípios básicos da segurança da informação, o princípio da confidencialidade, que diz que determinados arquivos e dados só podem ser acessados por pessoas autorizadas.

• FRAUDE INTERNA

São ataques maliciosos ou criminosos praticados pelos colaboradores da própria organização, o objetivo é roubar bens financeiros ou informações: dados de clientes, segredos comerciais e propriedade intelectual.

• INDISPONIBILIDADE

Ataques que causam a instabilidade ou queda dos sistemas organizacionais críticos afetando diretamente a imagem e o faturamento da empresa.

Como as empresas podem se preparar?

A implementação da norma ISO 27001 pode ser realizada utilizando os quatro passos do ciclo PDCA (Planejar, Executar, Controlar e Agir), podendo ou não ser gerenciado por outras metodologias mais específicas. A ISO 27001 deve ser vista como um projeto de implementação de um Sistema de Gestão da Segurança da Informação, abaixo estão alguns passos a serem seguidos:

- Obter apoio da Alta Direção
- Definir o escopo do SGSI
- Estabelecer a política de segurança da informação
- Definir a metodologia de avaliação de risco
- Realizar a avaliação de risco
- Elaborar a Declaração de Aplicabilidade
- Estabelecer o Plano de tratamento de risco
- Definir como medir a eficácia de seus controles e do seu SGSI
- Implementar todos os controles e procedimentos aplicáveis
- Implementar programas de treinamento e conscientização
- Realizar todas as operações diárias prescritas pela documentação do seu SGSI
- Monitorar e medir seu SGSI
- Realizar auditoria interna
- Realizar análise crítica pela direção
- Implementar ações corretivas

A certificação é resultado de um processo de adequação à ISO 27001 e as organizações precisam comprovar que estão em conformidade com as cláusulas obrigatórias da norma para serem certificadas. O projeto de implementação da ISO 27001 pode ser realizado apenas com os colaboradores da organização ou contar com o suporte de consultoria especializada.

A Norma 27001:2013 e a sua estrutura

A norma ISO 27001 é composta de 10 seções e 1 anexo (A). Destes, as seções de 0 a 3 são introdutórias e não implementáveis, das seções 4 a 10 estão contidos as obrigatoriedades e o Anexo A contempla um catálogo de 114 controles, cada um com seu objetivo e controle específico de segurança da informação, que são derivados diretamente e estão alinhados com a ISO 27002 - seções 5 a 15. Os objetivos e controles devem ser selecionados pela organização de acordo com o escopo e declaração de aplicabilidade (SOA) de um SGSI.

Os títulos das seções da ISO 27001 são os mesmos de outras normas de gestão, permitindo uma integração mais fácil destas normas, de acordo com o Anexo SL das Diretivas ISO / IEC da International Organization for Standardization.

4 Contexto da Organização

4.1 Compreender a Organização e seu Contexto

As questões internas e externas relevantes ao propósito da organização e que afetam sua capacidade de atingir os resultados pretendidos do seu SGSI precisam estar determinadas. É extremamente importante identificar o cenário ao qual a organização está inserida para definição do planejamento estratégico.

4.2 Entender as necessidades e expectativas das partes interessadas

A organização precisa identificar quem são suas partes interessadas, assim como suas necessidades e expectativas com relação ao Sistema de Gestão da Segurança da Informação. O entendimento das partes interessadas provê apoio na identificação de riscos e oportunidades. É importante considerar que possa existir outras partes interessadas relevantes para os SGSI, mas não somente relacionada a requisitos legais, elas podem, possivelmente, influenciar a segurança da informação dentro da sua organização, devido ao nível requerido de proteção da informação e as medidas de segurança adotadas.

4.3 Determinação do escopo do sistema de gestão da segurança da informação

A partir do entendimento de seu contexto, das necessidades de suas partes interessadas, , bem como as interfaces e dependências entre as atividades, processos ou funções desempenhadas pela organização e aquelas que são realizadas por outras organizações, o escopo do SGSI estará determinado. A determinação do escopo apoiará a organização a identificar seus processos principais e seus processos de apoio.

4.4 Sistema de gestão de segurança da informação

Como base para o sistema de gestão, será utilizado o PDCA – Planejamento, Operação, Checagem e Ação para todos os processos do SGSI.

5 Liderança

5.1 Liderança e compromisso

A alta Direção da organização deve identificar claramente o seu comprometimento com a implementação e manutenção do SGSI. Como evidencia de comprometimento, podemos destacar a elaboração da Política de Segurança da Informação e seus objetivos, a provisão de recursos, a motivação e capacitação dos colaboradores, entre outras.

5.2 Política

Estabelece as diretrizes do Sistema de Gestão da Segurança da Informação, ela precisa acompanhar o direcionamento estratégico da organização assim como referenciar os objetivos. A PSI estabelece também o comprometimento com o cumprimento dos requisitos legais e a melhoria contínua.

5.3 Papéis, responsabilidades e autoridades organizacionais

As organizações e as pessoas devem saber o que devem e o que não devem fazer. Para um SGSI eficaz os papeis, responsabilidades e autoridade precisam estar claramente definidas e conhecidas por todos na Organização, assegurando o bom funcionamento entre as diferentes áreas e a as suas pessoas.

6 Planejamento

6.1 Ações para endereçar os riscos e oportunidades

Priorizar as atividades e os processos do SGSI de acordo com seu impacto potencial nos resultados pretendidos e aproveitar as oportunidades identificadas.

É importante que a organização considere as questões internas e externas relevantes, incluindo as partes interessadas e seus requisitos para determinar os riscos e oportunidades que precisam ser considerados.

Um processo de avaliação de risco precisa ser definido para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade de informações no escopo do SGSI, bem como também as análises e avaliações dos riscos. Para cada risco identificado é necessário atribuí-lo a um proprietário, que será responsável por aceitar o tratamento de risco e o risco residual.

Um risco deriva de diferentes fontes e causas de risco (ameaças e vulnerabilidades). Cabe a organização analisar os potenciais consequências e impactos se o risco for materializado, bem como avaliar a probabilidade da ocorrência de um tal risco.

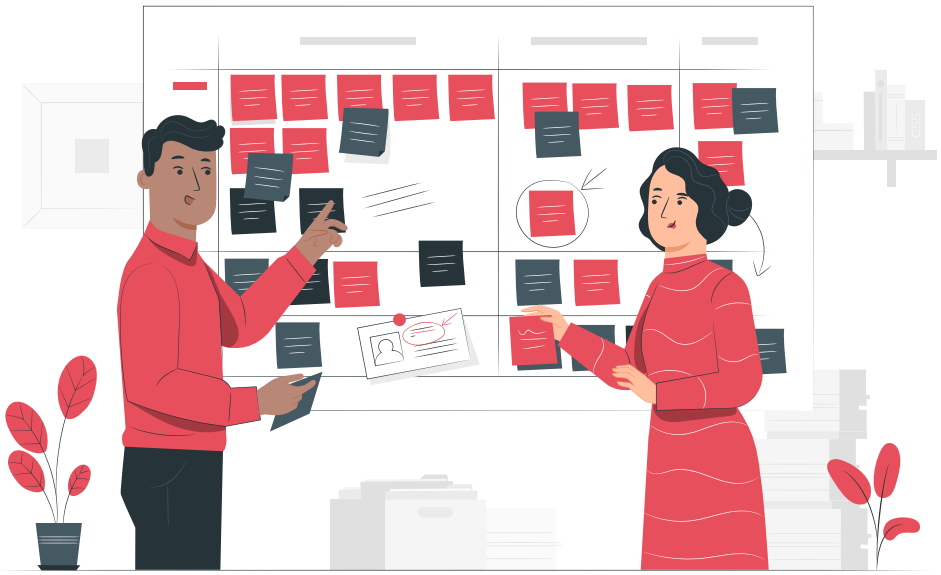
O processo de avaliação de risco compara a análise de riscos com os critérios de aceitação e priorizar as ações para o tratamento riscos.

A organização precisa selecionar a opção adequada de tratamento de risco e, em seguida, determinar todos os controles que são necessários. As opções de tratamento de riscos não são necessariamente exclusiva e podem incluir:

- Evitar o risco,
- Transferir o risco,
- Aceitar
- Mitigar

6.2 Objetivos da segurança de informações de e planos para alcançá-los

A organização deve estabelecer os objetivos do SGSI consistentes com os objetivos estratégicos. Eles devem estar alinhados com a PSI.



7 Suporte

7.1 Recursos

A organização precisa estabelecer e disponibilizar os recursos necessários para a operação e controle dos processos, para a garantia de conformidade aos requisitos de segurança da informação e eficácia do sistema.

7.2 Competência

A organização determina, desenvolve e assegura as competências das pessoas necessárias para o bom desempenho do SGSI. É fundamental que elas possuam competências consistentes com as funções, responsabilidades e autoridades atribuídas para poderem contribuir com o SGSI.

7.3 Conscientização

As pessoas que trabalham sob o controle da organização devem estar cientes da política de segurança da informação e como ela contribui para a eficácia do SGSI e as implicações no caso de não conformidade com os requisitos do SGSI.

7.4 Comunicação

É necessário estabelecer quais são as comunicações internas e externas relevantes para o SGSI, pois tem como objetivo facilitar o entendimento, alinhamento e a cooperação de todos para assegurar a implementação eficaz dos SGSI. A comunicação deve ser realizada entre os diversos níveis e funções dentro da organização.

7.5 Informações Documentadas

O conceito de informação documentada foi introduzido como parte da estrutura comum de nível alto (HLS) e nos termos comuns para normas de sistema de gestão enfatizando que a informação documentada independe de seu formato.

8 Operação

8.1 Planejamento Operacional e controle

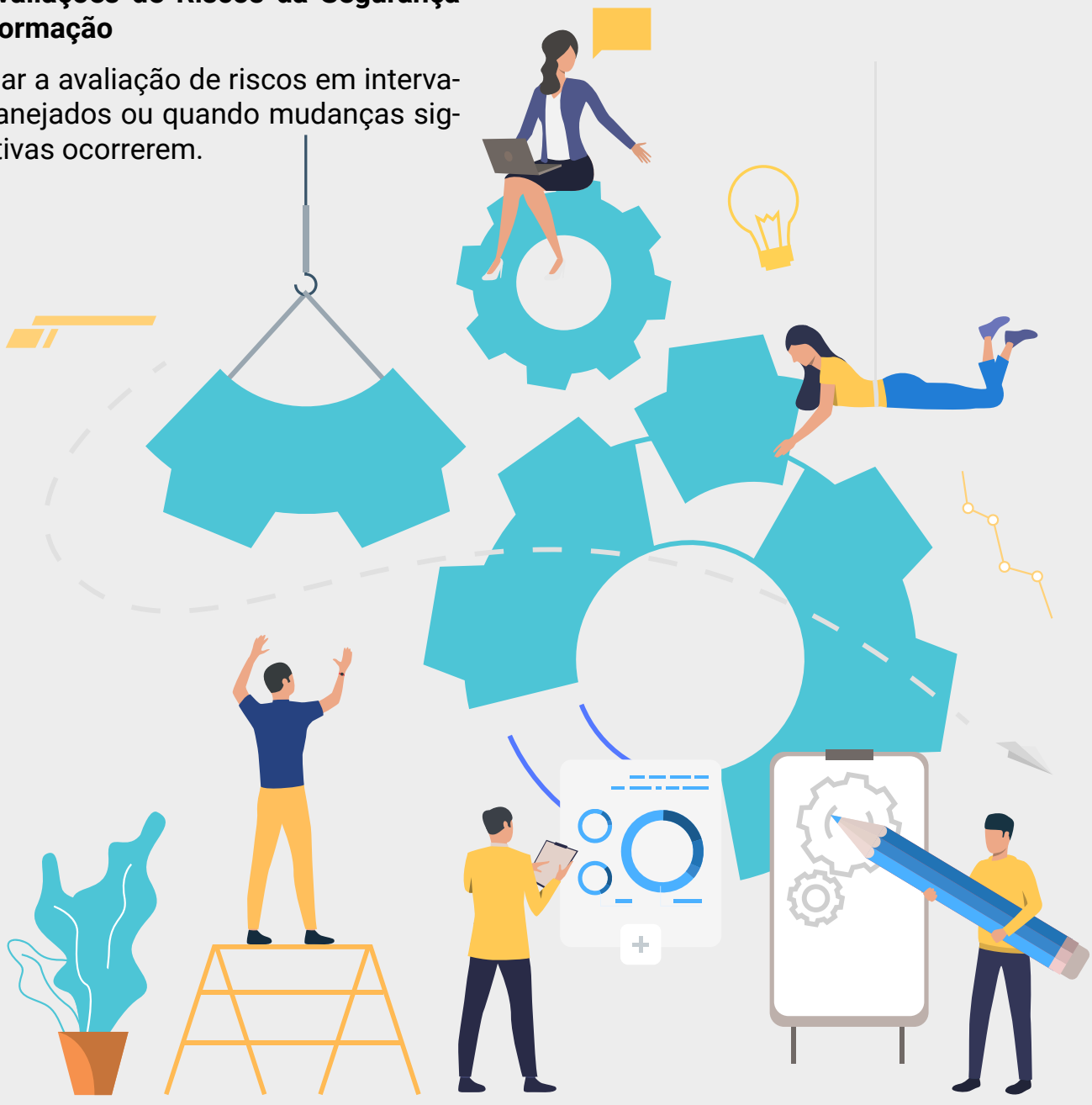
Planejar, implementar e controlar os processos necessários para atendimento aos requisitos do SGSI, controlar os processos terceirizados, além das mudanças planejadas e a sua análise crítica.

8.2 Avaliações de Riscos da Segurança da Informação

Realizar a avaliação de riscos em intervalos planejados ou quando mudanças significativas ocorrerem.

8.3 Tratamento de Riscos da Segurança da Informação

Implementação do plano de tratamento de riscos.



9 Avaliação de Desempenho

9.1 Monitoramento, medição, análise e avaliação

A organização determina os métodos de monitorização, medição, análise e avaliação adequados para obter informação válida sobre o desempenho do SGSI.

O desempenho e a eficácia do SGSI são alcançados na medida em que a organização fornece, consistentemente, produtos e serviços que satisfaçam tanto os requisitos do cliente como legais aplicáveis.

9.2 Auditorias internas

A organização assegura que são realizadas auditorias internas para avaliar a conformidade com as disposições planejadas e os requisitos da ISO 27001, determinando se o sistema está implementado e é mantido com eficácia.

As auditorias internas têm por finalidade avaliar o cumprimento dos requisitos da ISO 27001:2013, a adequação e implementação das políticas da organização, os procedimentos, instruções de trabalho e a eficácia dos processos em alcançar os objetivos traçados. Também permitem a identificação de oportunidades de melhoria, sendo um importante instrumento e um fator chave no ciclo PDCA para o SGSI da organização.

O programa de auditorias deve incluir

A frequência da auditoria, os métodos, as responsabilidades envolvidas, os requisitos de planejamento e de emissão de relatórios. Poderá partir de uma abordagem baseada no risco, e deverá considerar a situação, a importância e a complexidade dos processos, as áreas a serem auditadas, alterações que tenham ocorrido e que afetem a organização, bem como resultados das auditorias anteriores. É esperado inclusão, no programa de auditorias internas de processos ou atividades contratadas, caso tenham um impacto relevante nos resultados do SGSI.

9.3 Análises Críticas pela Alta Direção

A Alta Direção analisa criticamente os resultados da avaliação do desempenho do sistema, a sua eficácia, adequabilidade e o alinhamento com a estratégia organizacional para decidir sobre a necessidade de mudanças, ações de melhoria e respetivos recursos.

10 Melhoria

10.1 Não conformidades e ações corretivas

A organização promove ações de melhoria para atender aos requisitos dos clientes e aumentar a sua satisfação.

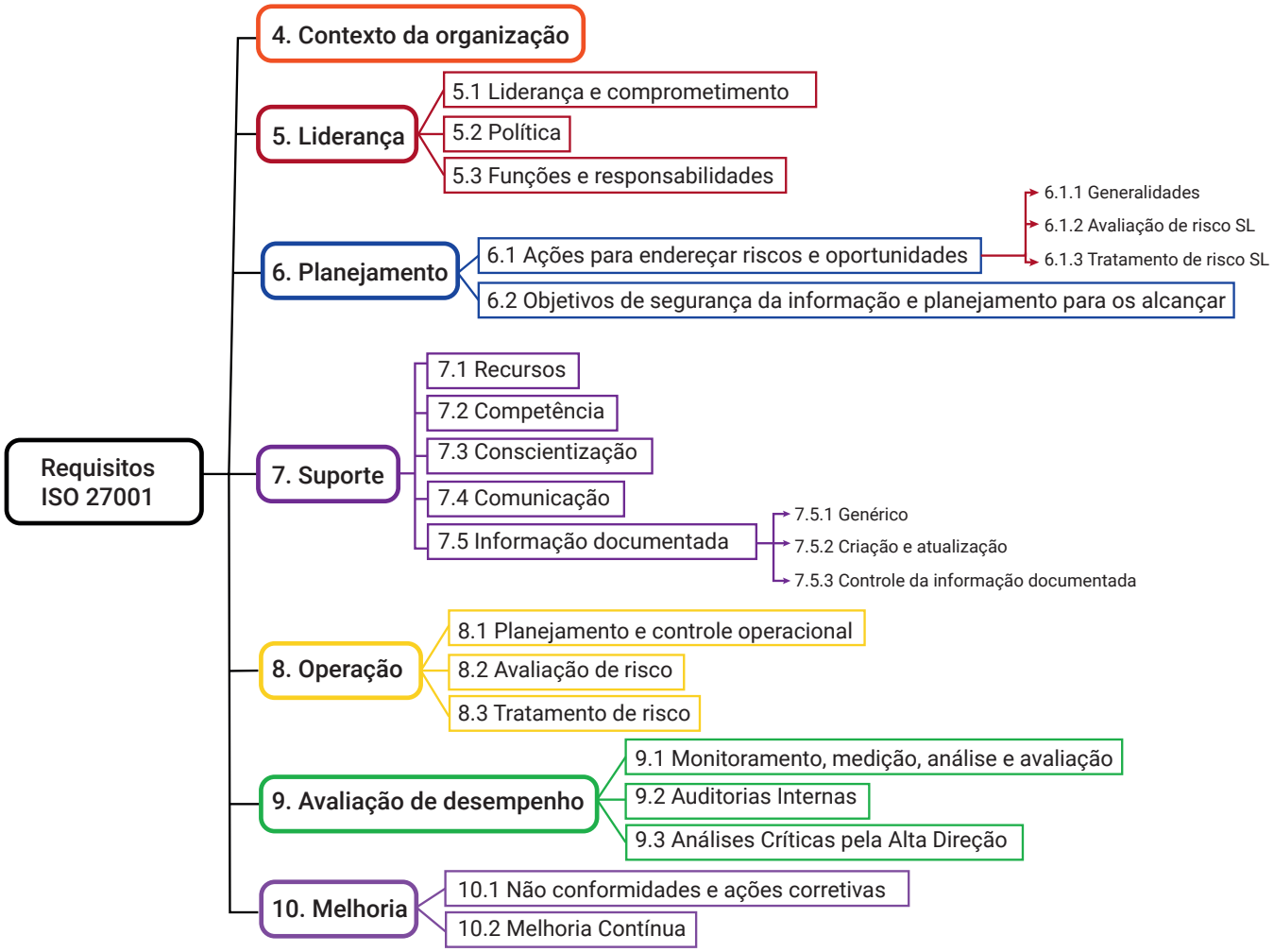
10.2 Melhoria Contínua

Uma não conformidade é um não atendimento a um requisito e a ação corretiva é a ação tomada para eliminar a causa de uma não conformidade e prevenir a sua repetição.

As não conformidades podem ser detectadas interna ou externamente, ter origem em reclamações de clientes, identificadas no controlo das saídas não conformes de processos, produtos e serviços ou em auditorias internas ou externas.

Quando ocorre uma não conformidade, a ISO 27001:2013 indica a primeira ação que é reagir a essa não conformidade. Isso implica em definir medidas para corrigir e controlar e para lidar com as consequências, na medida aplicável. Esta reação é comumente chamada de correção.

A organização identifica as falhas e não conformidades, corrige-as, investiga as causas e toma ações corretivas para prevenir a recorrência, assegurando a melhoria.



Anexo A da ISO 27001:2013

A.5 Política de Segurança

A.6 Organização da Segurança da Informação

A.7 Segurança em Recursos Humanos

A.8 Gestão de Ativos

A.9 Controle de Acesso

A.10 Criptografia

A.11 Segurança Física e do Ambiente

A.12 Segurança nas Operações

A.13 Segurança nas Comunicações

A.14 Aquisição, Desenvolvimento e Manutenção de Sistemas

A.15 Relacionamento na Cadeia de Suprimento

A.16 Gestão de Incidente de Segurança da Informação

A.17 Aspectos da Segurança da Informação na Gestão de Continuidade de Negócio

A.18 Conformidade / Compliance

Introdução - Define o propósito da ISO 27001 e sua compatibilidade com outras normas de gestão.

Escopo – explica que esta norma é aplicável a qualquer tipo de organização.

Referência normativa – refere-se a ISO / IEC 27000 como uma norma onde termos e definições são dados.

Termos e definições – novamente, refere-se a ISO / IEC 27000.

Contexto da organização – define requisitos para o entendimento de assuntos externos e internos, partes interessadas e seus requisitos, e a definição do escopo do SGSI. (etapa de planejamento (Plan) do ciclo PDCA)

Liderança – define as responsabilidades da Alta Direção, estabelecendo papéis e responsabilidades, e o conteúdo da política de segurança da informação de alto nível. (etapa de planejamento (Plan) do ciclo PDCA)

Planejamento – define requisitos para a avaliação de risco, plano de tratamento de risco, Declaração de Aplicabilidade e

define os objetivos de segurança da informação. (etapa de planejamento (Plan) do ciclo PDCA)

Apoio – define requisitos de disponibilidade de recursos, competências, conscientização, comunicação e controle de documentos e registros. (etapa de planejamento Plan) do ciclo PDCA)

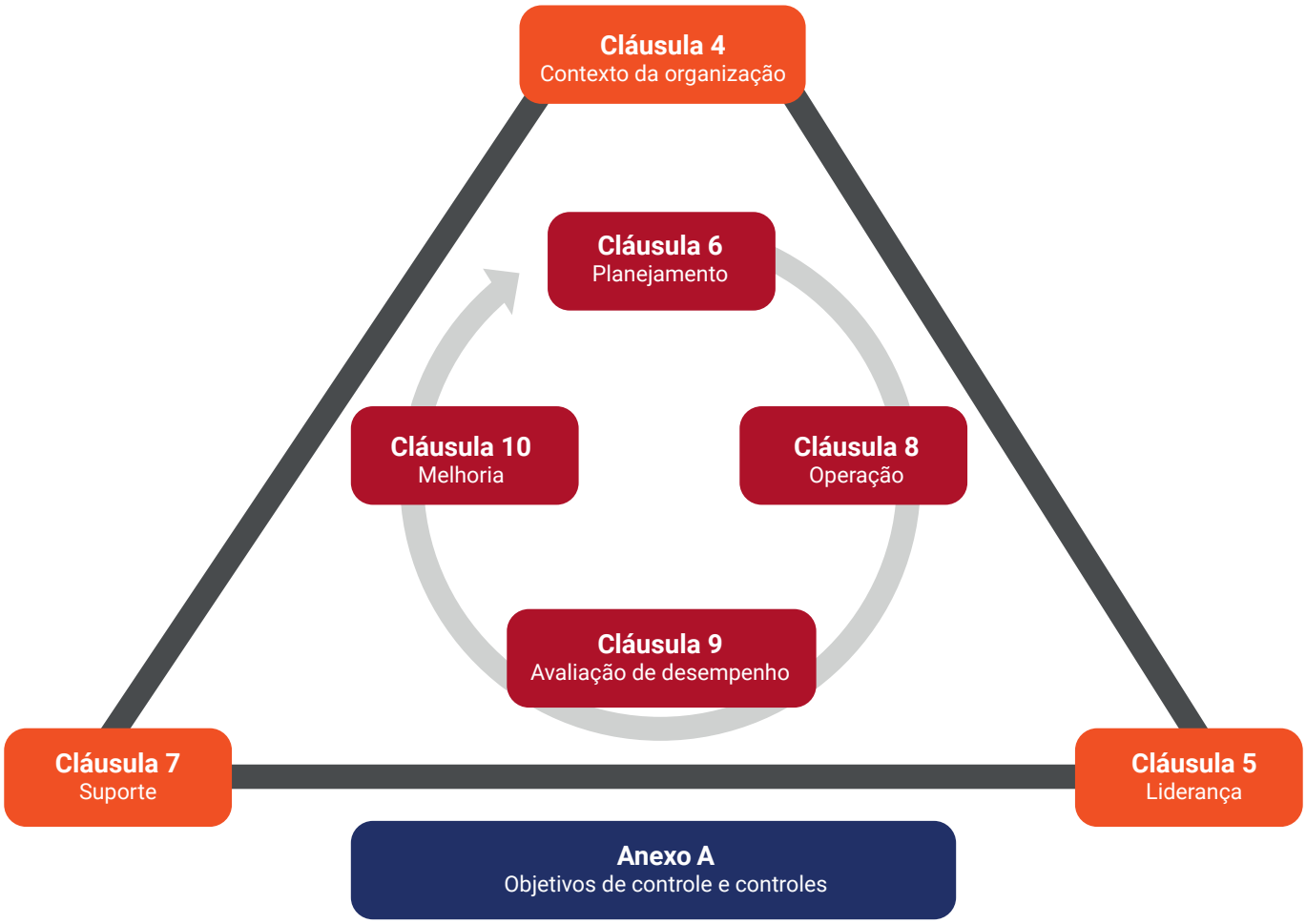
Operação – define a implementação da avaliação e tratamento de risco, assim como controles e outros processos necessários para atingir os objetivos de segurança da informação. (etapa execução (Do) do ciclo PDCA)

Avaliação do desempenho – define requisitos para o monitoramento, medição, análise, avaliação, auditoria interna e análise crítica pela Direção. (etapa verificação (Check) do ciclo PDCA)

Melhoria – define requisitos para não conformidades, ações corretivas e melhoria contínua. (etapa de atuação (Act) do ciclo PDCA)

Anexo A – este anexo disponibiliza um catálogo de 114 controles (salvaguardas) distribuídos em 14 seções (seções de A.5 até A.18).

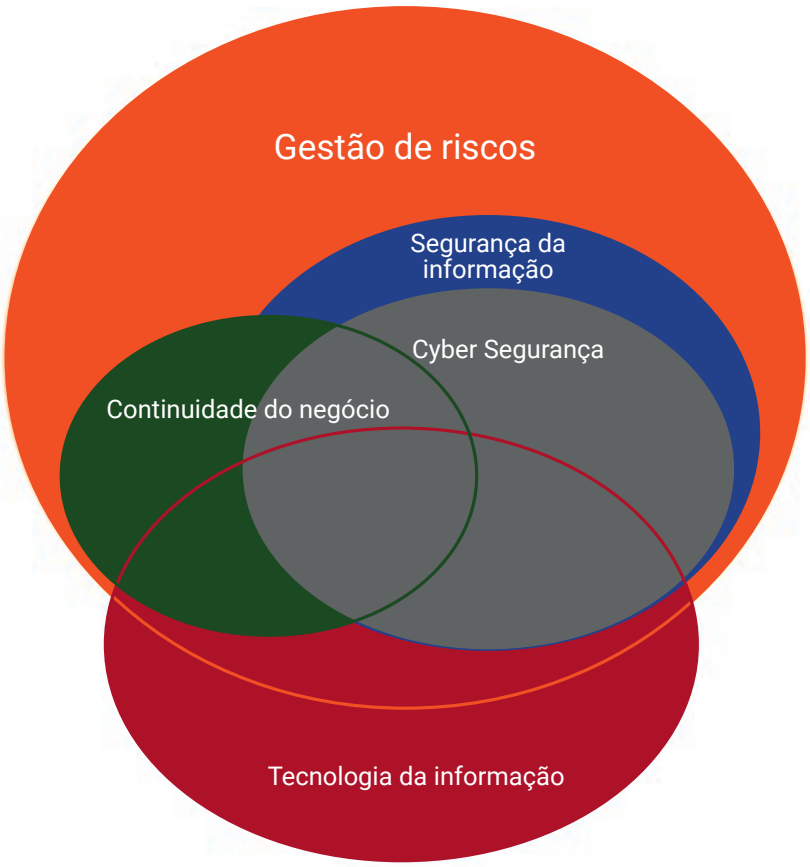
A estrutura da ISO 27001 pode ser representada da seguinte forma:



A norma ISO 27001:2013

A ISO 27001 é uma norma de apoio para implementação de um sistema de gestão de segurança da informação (SGSI) que protege os ativos de informação, identificando potenciais problemas e definindo ações para prevenir que esses problemas ocorram, reduzindo risco e tempo de parada. O foco da ISO 27001 é proteger confidencialidade, integridade e disponibilidade de informações de uma organização.

A gestão de riscos é parte fundamental para segurança da informação em uma organização, com sobreposição em áreas de cyber segurança, gestão da continuidade do negócio e gestão de TI conforme a ilustração abaixo.



A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela também possibilita que organizações obtenham certificação, o que significa que: organizações certificadas serão capazes de demonstrar aos órgãos reguladores, clientes e partes interessadas que estão em conformidade com os requisitos da norma e melhores práticas no que diz respeito à segurança da informação.

Imagina-se que implementação de um SGSI gerará altos custos e oferecendo pouco retorno financeiro, mas a verdade é que os custos serão compensados pela prevenção e redução do impacto dos incidentes de segurança.

Princípios do Sistema de Segurança da Informação

Para proteger as informações, a segurança da informação se baseia em três pilares: Confidencialidade, Integridade e Disponibilidade.

1. Princípio da Disponibilidade

A disponibilidade está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas da organização, esse princípio é de suma importância, pois, falhas de indisponibilidade comprometem o serviço prestado pela organização.

Através dos riscos associados a informação mapeados, a organização deve criar um plano de recuperação de dados, com um Plano de Continuidade de Negócios e recuperação de desastres (Disaster Recover), que serão colocados em prática de forma reativa a um incidente de segurança da informação.

2. Princípio da Integridade

Integridade é que garante a veracidade da informação e restringe o acesso e/ou alteração da informação por pessoas não autorizadas, garante a completude e preservação da precisão da informação, para que não haja perda de partes da informação.

3. Princípio da Confidencialidade

A confidencialidade é o que garante o sigilo de informação e impede que elas não sejam roubadas ou acessadas por pessoas não autorizadas.

Principais benefícios da implementação da norma ISO 27001:2013

- Reduzir de custos com tratamento de incidentes de segurança da informação.
- Maior credibilidade da marca, pois demonstra preocupação com os dados do cliente.
- Risco gerenciado por políticas de segurança claras e documentadas.
- Conformidade com requisitos legais.
- Melhor organização.
- Mitigação de riscos e redução do impacto das ocorrências;
- Ágil adaptação, pois as informações estão documentadas e são facilmente gerenciadas;
- Ganhos para a organização interna, fluxos processuais e otimização da gestão;
- Vantagem competitiva frente à concorrência.

Diante das crescentes ameaças à segurança da informação, a certificação ISO 27001 é um atestado que sua empresa está em conformidade com os requisitos da norma e possui uma boa gestão da segurança da informação.

A norma ISO 27701:2020

A norma ISO 27701 especifica requisitos relacionados ao SGPI (Sistema de Gestão da Privacidade da Informação) e diretrizes para os *controladores* e *operadores* de dados pessoais, atores com grandes responsabilidades no tratamento de dados. A ISO 27701 é uma extensão dos requisitos da ISO 27001 e de diretrizes da 27002, todos focados em privacidade da informação e complementando as demais normas de segurança da informação com seus requisitos específicos.

Para compreensão da ISO 27701 é preciso ter em mente que ela se relaciona a todo instante com as normas de segurança da informação.

Seção 1 – explica que esta norma é aplicável a qualquer tipo de organização.

Seção 2 – Refere-se a ISO/IEC 27000, a ISO/IEC 27001, a ISO/IEC 27002 e ISO/IEC 29100 como referências normativas.

Seção 3 – Refere-se a ISO/IEC 27000 e ISO/IEC 29100 como uma norma de termos e definições.

Seção 4 – Refere-se a ISO/IEC 27001 e ISO/IEC 27002 para detalhar a estrutura do documento.

Seção 5 - Define requisitos específicos de um sistema de gestão de privacidade da informação, de acordo com a ISO/IEC 27001.

Seção 6 – Define diretrizes específicas de um sistema de gestão de privacidade da informação, de acordo com a ISO/IEC 27002.

Seção 7 - Define as diretrizes para controladores.

Seção 8 – Define as diretrizes para operadores.

Anexo A – Uma lista de controles para controladores de DP. (Normativo)

Anexo B – Uma lista de controles para operadores de DP. (Normativo)

Anexo C – Mapeamento de controles para controladores de DP com os princípios da privacidade da ISO/IEC 29100. (Informativo)

Anexo D - Mapeamento de cláusulas da ISO/IEC 27701 com os artigos do GDPR (5 a 49 exceto 43). (Informativo)

Anexo E - Mapeamento de cláusulas da ISO/IEC 27701 com os requisitos da ISSO/IEC 27018 para operadores de DP em nuvens públicas e ISO/IEC 29151 para controles e orientações adicionais para controladores de DP. (Informativo)

Anexo F – Detalhes sobre como aplicar a ISO/IEC 27701 com ISO/IEC 27001 e ISO/IEC 27002. (Informativo)

Anexo N/A – Mapeamento com a LGPD. (Informativo)

Assim como a ISO 27001, a organização deve selecionar os controles aplicáveis de acordo com o escopo e avaliação de riscos a ser realizada. Porém, a exclusão de qualquer controle deverá ser justificada na declaração de aplicabilidade (SOA).

Outro item importante é o mapeamento entre a GDPR (General Data Protection Regulation) e LGPD (Lei Geral de Proteção de Dados), respectivamente nos Anexos D e N/A. Neste ponto, podemos observar claramente a aderência aos requisitos e controles da norma podem ser relevantes para o cumprimento da maior parte das obrigações previstas nas Leis.

Princípios do Sistema de Gestão de Privacidade

Assim como a ISO 27001, a ISO 27701 visa proteger as informações e o conjunto de valores compartilhados, governando a proteção de privacidade de dados pessoais (DP), quando tratados em sistemas de tecnologia da informação e comunicação. Ela se baseia em 5 pilares, além dos três pilares da ISO 27001: Confidencialidade, Integridade, Disponibilidade e agregou-se mais dois pilares: o tratamento de dados pessoais e a proteção da privacidade.

1. Princípio do tratamento de dados pessoais

Operação ou conjunto de operações realizadas sobre dados pessoais. (Ciclo de vida dos dados) Exemplos de operações de tratamento de DP incluem, mas não estão limitados a coleta, armazenamento, alteração, recuperação, consulta, divulgação, anonimização, pseudoanimização, disseminação ou disponibilização, exclusão ou destruição de DP.

2. Princípio da proteção da privacidade

Conjunto de valores compartilhados, governando a proteção de privacidade de dados pessoais (DP), quando tratados em sistemas de tecnologia da informação e comunicação.

A norma ISO 27701:2020 e a sua estrutura comparada a ISO 27001:2013

Os requisitos da ISO 27001:2013 mencionando "segurança da informação" devem ser estendidos para a proteção de privacidade, caso esta seja potencialmente afetada pelo tratamento de DP.

Como as demais normas de sistemas de gestão são a ISO 27701 é dividida em 10 cláusulas, sendo que as 5 primeiras são introdutórias e remetem para requisitos genéricos como Introdução, Escopo, Referência Normativa e Termos e Definições e apresentação da estrutura dos documentos. A seguir vamos apresentar com mais detalhes as clausulas específicas do Sistema de Gestão sua comparação com a ISO 27001.

ISO 27001	TÍTULO	ISO 27701	OBSERVAÇÕES ADICIONAIS
4	Contexto da Organização	5.2	Requisitos adicionais 5.2.2 Determinar o papel da organização domo controlador e/ou operador de dado pessoal 5.2.3 Incluir o tratamento do dado pessoal na determinação do escopo do SGPI 5.2.4 Estabelecer, implementar, manter e melhorar continuamente um SGPI de acordo com os requisitos da ISO 27001:2013, seções 4 a 10, estendidos pelos requisitos da seção 5.
5	Liderança	5.3	Sem requisitos específicos de SGPI
6	Planejamento	5.4	Requisitos adicionais - 5.4.1.2 – Avaliação do Riscos de Segurança da Informação - Aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, dentro do escopo do SGPI. - Aplicar o processo de avaliação de riscos de privacidade para identificar os riscos relativos ao tratamento de DP, dentro do escopo do SGPI. - Os objetivos de controle e dos controles da ISO27001:2013, Anexo A, para o tratamento dos riscos, os objetivos de controles e os controles devem ser consi-de¬rados no contexto de ambos os riscos de segurança da informação, bem como os riscos relativos ao tratamento de DP, incluindo os riscos dos titulares de DP.
7	Apoio	5.5	Sem requisitos específicos de SGPI
8	Operação	5.6	Sem requisitos específicos de SGPI
9	Avaliação de Desempenho	5.7	Sem requisitos específicos de SGPI
10	Melhoria	5.8	Sem requisitos específicos de SGPI

4 Geral

4.1 Estrutura deste documento -

4.2 Aplicação dos requisitos da ABNT NBR ISO/IEC 27001:2013

4.3 Aplicação das diretrizes da ABNT NBR ISO/IEC 27002:2013

4.4 Cliente

5 Requisitos específicos de SGPI relacionados à ABNT NBR ISO/IEC 27001

5.1 Geral

5.2 Contexto da organização

5.2.1 Entendendo a organização e seu contexto – Neste

5.2.2 Entendendo as necessidades e as expectativas das partes interessadas

5.2.3 Determinando o escopo do sistema de gestão da segurança da informação

5.2.4 Sistema de gestão da segurança da informação

5.3 Liderança

5.3.1 Liderança e comprometimento

5.3.2 Política

5.3.3 Autoridades, responsabilidades e papéis organizacionais

5.4 Planejamento

5.4.1 Ações para contemplar riscos e oportunidades

5.4.2 Objetivos de segurança da informação e planejamento para alcançá-los

5.5 Apoio

5.5.1 Recursos

5.5.2 Competência

5.5.3 Conscientização

5.5.4 Comunicação

5.5.5 Informação documentada

5.5.5.1 Geral

5.5.5.2 Criando e atualizando

5.5.5.3 Controle da informação documentada

5.6 Operação

5.6.1 Planejamento e controle operacional

5.6.2 Avaliação de riscos de segurança da informação

5.6.3 Tratamento de riscos de segurança da informação

5.7 Avaliação de desempenho

5.7.1 Monitoramento, medição, análise e avaliação

5.7.2 Auditoria interna

5.7.3 Análise crítica pela Direção

5.8 Melhoria

5.8.1 Não conformidade e ação corretiva

5.8.2 Melhoria contínua

6 Diretrizes específicas de SGPI relacionadas à ABNT NBR ISO/IEC 27002

6.1 Geral

6.2 Políticas de segurança da informação

6.2.1 Orientação da Direção para segurança da informação

6.2.1.1 Políticas para segurança da informação

6.2.1.2 Análise crítica das políticas para segurança da informação

6.3 Organização da segurança da informação

6.3.1 Organização interna

6.3.1.1 Responsabilidades e papéis da segurança da informação

6.3.1.2 Segregação de funções

6.3.1.3 Contato com autoridades

6.3.1.4 Contato com grupos especiais

6.3.1.5 Segurança da informação no gerenciamento de projetos

6.3.2 Dispositivos móveis e trabalho remoto

6.3.2.1 Política para o uso de dispositivo móvel

6.4 Segurança em recursos humanos

6.4.1 Antes da contratação

6.4.1.1 Seleção

6.4.1.2 Termos e condições de contratação

6.4.2 Durante a contratação

6.4.2.1 Responsabilidades da Direção

6.4.2.2 Conscientização, educação e treinamento em segurança da informação

6.4.2.3 Procedimentos disciplinares

6.4.3 Encerramento e mudança da contratação

6.4.3.1 Responsabilidades pelo encerramento ou mudança da contratação

6.5 Gestão de ativos

6.5.1 Responsabilidade pelos ativos

6.5.1.1 Inventário dos ativos

6.5.1.2 Proprietário dos ativos

6.5.1.3 Uso aceitável dos ativos

6.5.1.4 Devolução de ativos

6.5.2 Classificação da informação

6.5.2.1 Classificação da informação

6.5.2.2 Rótulos e tratamento da informação

6.5.2.3 Tratamento dos ativos

6.5.3 Tratamento de mídias

6.5.3.1 Gerenciamento de mídias removíveis

6.5.3.2 Descarte de mídias

6.5.3.3 Transferência física de mídias

6.6 Controle de acesso

6.6.1 Requisitos do negócio para controle de acesso

6.6.1.1 Política de controle de acesso

6.6.1.2 Acesso às redes e aos serviços de rede

6.6.2 Gerenciamento de acesso do usuário

6.6.2.1 Registro e cancelamento de usuário

6.6.2.2 Provisionamento para acesso de usuário

6.6.2.3 Gerenciamento de direitos de acesso privilegiado

6.6.2.4 Gerenciamento da informação de autenticação secreta de usuários

6.6.2.5 Análise crítica dos direitos de acesso de usuário

6.6.2.6 Retirada ou ajuste dos direitos de acesso

6.6.3 Responsabilidades dos usuários

6.6.3.1 Uso da informação de autenticação secreta

6.6.4 Controle de acesso ao sistema e

à aplicação

6.6.4.1 Restrição de acesso à informação

6.6.4.2 Procedimentos seguros de entrada no sistema (log-on)

6.6.4.3 Sistema de gerenciamento de senha

6.6.4.4 Uso de programas utilitários privilegiados

6.6.4.5 Controle de acesso ao código-fonte de programas

6.7 Criptografia

6.7.1 Controles criptográficos

6.7.1.1 Política para o uso de controles criptográficos

6.7.1.2 Gerenciamento de chaves

6.8 Segurança física e do ambiente

6.8.1 Áreas seguras

6.8.1.1 Perímetro de segurança física

6.8.1.2 Controles de entrada física

6.8.1.3 Segurança em escritórios, salas e instalações

6.8.1.4 Proteção contra ameaças externas e do meio ambiente

6.8.1.5 Trabalhando em áreas seguras

6.8.1.6 Áreas de entrega e de carregamento

6.8.2 Equipamentos

6.8.2.1 Localização e proteção do equipamento

6.8.2.2 Utilidades

6.8.2.3 Segurança do cabeamento

6.8.2.4 Manutenção dos equipamentos

6.8.2.5 Remoção de ativos

6.8.2.6 Segurança de equipamentos e ativos fora das dependências da organização

6.8.2.7 Reutilização ou descarte seguro de equipamentos

6.8.2.8 Equipamento de usuário sem monitoração

6.8.2.9 Política de mesa limpa e tela limpa

6.9 Segurança nas operações

6.9.1 Responsabilidades e procedimentos operacionais

6.9.1.1 Documentação dos procedimentos de operação

6.9.1.2 Gestão de mudanças

6.9.1.3 Gestão de capacidade

6.9.1.4 Separação dos ambientes de desenvolvimento, teste e de produção

6.9.2 Proteção contra códigos maliciosos

6.9.2.1 Controles contra códigos maliciosos

6.9.3 Cópias de segurança

6.9.3.1 Cópias de segurança das informações

6.9.4 Registros e monitoramento

6.9.4.1 Registros de eventos (logs)

6.9.4.2 Proteção das informações dos registros de eventos (logs)

6.9.4.3 Registros de eventos (log) de administrador e operador

6.9.4.4 Sincronização dos relógios

6.9.5 Controle de software operacional

6.9.5.1 Instalação de software nos sistemas operacionais

6.9.6 Gestão de vulnerabilidades técnicas

6.9.6.1 Gestão de vulnerabilidades técnicas

6.9.6.2 Restrições quanto à instalação de software

6.9.7 Considerações quanto à auditoria de sistemas de informação

6.9.7.1 Controles de auditoria de sistemas de informação

6.10 Segurança nas comunicações

6.10.1 Gerenciamento da segurança em redes

6.10.1.1 Controles de redes

6.10.1.2 Segurança dos serviços de rede

6.10.1.3 Segregação de redes

6.10.2 Transferência de informação

6.10.2.1 Políticas e procedimentos para transferência de informações

6.10.2.2 Acordos para transferência de informações

6.10.2.3 Mensagens eletrônicas

6.10.2.4 Acordos de confidencialidade e não divulgação

6.11 Aquisição, desenvolvimento e manutenção de sistemas

6.11.1 Requisitos de segurança de sistemas de informação

6.11.1.1 Análise e especificação dos requisitos de segurança da informação

6.11.1.2 Serviços de aplicação seguros em redes públicas

6.11.1.3 Protegendo as transações nos aplicativos de serviços

6.11.2 Segurança em processos de desenvolvimento e de suporte

6.11.2.1 Política de desenvolvimento seguro

6.11.2.2 Procedimentos para controle de mudanças de sistemas

6.11.2.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais

6.11.2.4 Restrições sobre mudanças em pacotes de software

6.11.2.5 Princípios para projetar sistemas seguros

6.11.2.6 Ambiente seguro para desenvolvimento

6.11.2.7 Desenvolvimento terceirizado

6.11.2.8 Teste de segurança do sistema

6.11.2.9 Teste de aceitação de sistemas

6.11.3 Dados para teste

6.11.3.1 Proteção dos dados para teste

6.12 Relacionamento na cadeia de suprimento

6.12.1 Segurança da informação na cadeia de suprimento

6.12.1.1 Política de segurança da informação no relacionamento com os fornecedores

6.12.1.2 Identificando segurança da informação nos acordos com fornecedores

6.12.1.3 Cadeia de suprimento na tecnologia da informação e comunicação

6.12.2 Gerenciamento da entrega do serviço do fornecedor

6.12.2.1 Monitoramento e análise crítica de serviços com fornecedores

6.12.2.2 Gerenciamento de mudanças para serviços com fornecedores

6.13 Gestão de incidentes de segurança da informação

6.13.1 Gestão de incidentes de segurança da informação e melhorias

6.13.1.1 Responsabilidades e procedimentos

6.13.1.2 Notificação de eventos de segurança da informação

6.13.1.3 Notificando fragilidades de segurança da informação

6.13.1.4 Avaliação e decisão dos eventos de segurança da informação

6.13.1.5 Resposta aos incidentes de segurança da informação

6.13.1.6 Aprendendo com os incidentes de segurança da informação

6.13.1.7 Coleta de evidências

6.14 Aspectos da segurança da informação na gestão da continuidade do negócio

6.14.1 Continuidade da segurança da informação

6.14.1.1 Planejando a continuidade da segurança da informação

6.14.1.2 Implementando a continuidade da segurança da informação

6.14.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação

6.14.2 Redundâncias

6.14.2.1 Disponibilidade dos recursos de processamento da informação

6.15 Compliance

6.15.1 Compliance com requisitos legais e contratuais

6.15.1.1 Identificação da legislação aplicável e de requisitos contratuais

6.15.1.2 Direitos de propriedade intelectual

6.15.1.3 Proteção de registros

6.15.1.4 Proteção e privacidade de DP

6.15.1.5 Regulamentação de controles de criptografia

6.15.2 Análise crítica da segurança da informação

6.15.2.1 Análise crítica independente da segurança da informação

6.15.2.2 Compliance com as políticas e normas de segurança da informação

6.15.2.3 Análise crítica técnica do compliance

7 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para controladores de DP

7.1 Geral

7.2 Condições para coleta e tratamento

7.2.1 Identificação e documentação do propósito

7.2.2 Identificação de bases legais

7.2.3 Determinando quando e como o consentimento deve ser obtido

7.2.4 Obtendo e registrando o consentimento

7.2.5 Avaliação de impacto de privacidade

7.2.6 Contratos com operadores de DP

7.2.7 Controlador conjunto de DP

7.2.8 Registros relativos ao tratamento de DP

7.3 Obrigações dos titulares de DP

7.3.1 Determinando e cumprindo as obrigações para os titulares de DP

7.3.2 Determinando as informações para os titulares de DP

7.3.3 Fornecendo informações aos titulares de DP

7.3.4 Fornecendo mecanismos para modificar ou cancelar o consentimento

7.3.5 Fornecendo mecanismos para negar o consentimento ao tratamento de DP

7.3.6 Acesso, correção e/ou exclusão

7.3.7 Obrigações dos controladores de DP para informar aos terceiros

7.3.8 Fornecendo cópia do DP tratado

7.3.9 Tratamento de solicitações

7.3.10 Tomada de decisão automatizada

7.4 Privacy by Design e Privacy by Default

7.4.1 Limite de coleta

7.4.2 Limite de tratamento

7.4.3 Precisão e qualidade

7.4.4 Objetivos de minimização de DP

7.4.5 Anonimização e exclusão de DP ao final do tratamento

7.4.6 Arquivos temporários

7.4.7 Retenção

7.4.8 Descarte

7.4.9 Controle de transmissão de DP

7.5 Compartilhamento, transferência e divulgação de DP

7.5.1 Identificando as bases para a transferência de DP entre jurisdições

7.5.2 Países e organizações internacionais para os quais os DP podem ser transferidos

7.5.3 Registros de transferência de DP

7.5.4 Registro de divulgação de DP para terceiros

8 Diretrizes adicionais da ABNT NBR ISO/IEC 27002 para os processadores de DP

8.1 Geral

8.2 Condições para coleta e tratamento

8.2.1 Acordos com o cliente

8.2.2 Propósitos da organização

8.2.3 Uso de marketing e propaganda

8.2.4 Violando instruções

8.2.5 Obrigações do cliente

8.2.6 Registros relativos ao tratamento de DP

8.3 Obrigações para os titulares de DP

8.3.1 Obrigações para os titulares de DP

8.4 Privacy by design e privacy by default

8.4.1 Arquivos temporários

8.4.2 Retorno, transferência ou descarte de DP

8.4.3 Controles de transmissão de DP

8.5 Compartilhamento, transferência e divulgação de DP

8.5.1 Bases para a transferência de DP entre jurisdições

8.5.2 Países e organizações internacionais para os quais DP podem ser transferidos

8.5.3 Registros de DP divulgados para terceiros

8.5.4 Notificação de solicitações de divulgação de DP

8.5.5 Divulgações legalmente obrigatórias de DP

8.5.6 Divulgação de subcontratados usados para tratar DP

8.5.7 Contratação de um subcontratado para tratar DP

8.5.8 Mudança de subcontratado para tratar DP

Anexo A – Uma lista de controles para controladores de DP. (Normativo)

Anexo B – Uma lista de controles para processadores de DP. (Normativo)

Anexo C – Mapeamento de controles para controladores de DP com os princípios da privacidade da ISO/IEC 29100. (Informativo)

Anexo D - Mapeamento de cláusulas da ISO/IEC 27701 com os artigos do GDPR (5 a 49 exceto 43). (Informativo)

Anexo E - Mapeamento de cláusulas da ISO/IEC 27701 com os requisitos da ISSO/IEC 27018 para operadores de DP em nuvens públicas e ISO/IEC 29151 para controles e orientações adicionais para controladores de DP. (Informativo)

Anexo F – Detalhes sobre como aplicar a ISO/IEC 27701 com ISO/IEC 27001 e ISO/IEC 27002. (Informativo)

Anexo N/A – Mapeamento com a LGPD. (Informativo)

Principais benefícios da implementação da norma ISO 27701:2019

• Demonstra para partes interessadas que a organização tem a preocupação com os dados e informações deles, gerando aumento da confiança;

• Atende as principais exigências da LGPD e GDPR;

• Foco nas responsabilidades dos colaboradores sobre a segurança e privacidade dos dados;

• Melhora os processos internos, diminuindo os riscos de vazamentos de dados.

• Traz transparência nos controles estabelecidos para gestão da privacidade.

• Aumento da competitividade.

• Integração com o Sistema de Gestão da Segurança da Informação.

• Redução de custo através da prevenção de incidentes de segurança da informação e privacidade.

Como funciona o processo de certificação?

Etapa 1 – Opção por contratar um consultor ou implementar internamente

Quando da decisão da empresa por ser certificar na ISO 27001 e ISO 27701, é necessária uma condução para esse projeto acontecer. A empresa pode optar por contratar um consultor com expertise nas Normas e em sistemas de gestão para orientação e condução do processo. Porém, esse fator não é mandatório, caso a empresa tenha profissionais com conhecimento nas Normas, ou queiram capacitar uma equipe interna, a implementação pode ser feita pela própria empresa.

Etapa 2 – Gap Analysis / Pré-Auditoria

Antes de iniciar o processo de auditoria oficial, ou enquanto o sistema de gestão ainda está em desenvolvimento, o cliente pode solicitar um gap analysis ou pré-auditoria para QMS. A QMS, como organismo de certificação, realizada uma visita com uma amostragem menor do que a auditoria de certificação, mas que as técnicas de auditoria são utilizadas para observar as deficiências (gaps) do sistema de gestão ou parte dele. Embora os resultados não são detalhados em relação às ações corretivas, uma lista de observações é preparada e entregue para o cliente no final do processo, bem como um relatório completo de conformidades.

Etapa 3 – Auditoria Inicial de Fase 1 e Fase 2

A auditoria de certificação inicial é dividida em duas fases, fase 1 e fase 2, a fase 1 é uma auditoria predominantemente documental para verificar se o sistema de gestão têm condições de ser auditado em uma auditoria de certificação fase 2, é nesse fase também que o plano de auditoria da fase 2 é elaborado.

A auditoria inicial de fase 2 é uma auditoria onde todas as técnicas de auditoria são aplicadas, com verificação documental, entrevistas, avaliação de processos, avaliação de infraestrutura, etc. Essa auditoria possui a maior quantidade de dias de auditoria e consequentemente a maior amostragem do ciclo de certificação. Ao final dessa fase o auditor já informa a empresa em reunião de fechamento a conclusão dos trabalhos e a recomendação ou não da certificação. Caso recomentado o certificado é enviado no prazo informado, caso não ações serão necessárias.

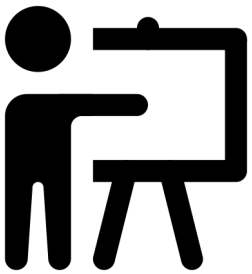
Etapa 4 – Auditorias de manutenção

Anualmente a QMS volta na empresa para verificar a adequação do sistema de gestão com as Normas aplicáveis em uma auditoria de manutenção, e ao final dos 3 anos (validado do certificado) uma auditoria de recertificação é necessária, obedecendo a mesma carga da auditoria de fase 2.

O que a QMS pode fazer para sua empresa nesse processo?

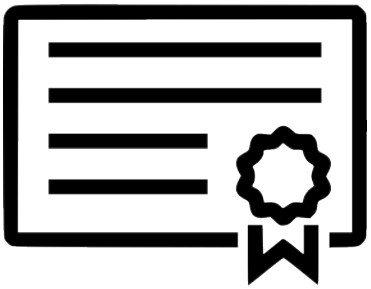
AUDITORIA DE ANÁLISE DE GAP

Avaliação dos seus processos conforme padrão ISO 27001 e ISO 27701 por audito¬res especializados a fim de observar lacunas para uma certificação.



TREINAMENTOS

Treinamento na sua empresa com instrutores especialistas sobre em ISO 27001 e ISO 27001, ou treina-mentos abertos em uma de nossas turmas (ver programação).



CERTIFICAÇÃO

Caso sua empresa ainda não seja certificada pela QMS, transfira sua certificação ou certifique conosco e tenha o melhor atendimento do mercado.

MAIS QUE UMA CERTIFICADORA, SEU VERDADEIRO PARCEIRO DE NEGÓCIOS.

SILVANA PONCE

QMS
Certification
Services

QMS Certification Services

contato@qmsbrasil.com.br
Av.Fagundes Filho, 145 cj.31
Saúde - São Paulo - SP
www.qmsbrasil.com.br