**ISO 27001**

**Um Sistema de Gestão de Segurança da Informação (SGSI)** - É um sistema de gestão corporativo voltado para a Segurança da Informação, que inclui toda a abordagem organizacional usada para proteger a informação empresarial e seus critérios de Confidencialidade, Integridade e Disponibilidade. O SGSI inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. A politica do SGSI é um documento de extrema importância e deve ter a aprovação e apoio da alta direção, a nível estratégico da organização. A organização deve comunicar as ações e melhorias do SGSI a todas as partes interessadas, com um nível de detalhamento apropriado às circunstâncias, bem como deve assegurar-se de que as melhorias atinjam os objetivos pretendidos. O processo do Sistema de Gestão de Segurança da Informação (SGSI), estabelecido pela norma NBR ISO/IEC 27001:2006, se baseia no modelo PDCA (plan do check act). Obs..: ISO/IEC 27002 "abandonou" o PDCA.

**Segundo a ISO 27001:2013,0.1** Geral, "A adoção de um SGSI é uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. São esperados que todos estes fatores de influência mudem ao longo do tempo."

Ao Implementar um modelo de SGSI em uma organização significa construir uma sistemática abrangente, integrada e contínua, para minimizar ricos associados a informação. A NBR ISO/ IEC 27001 incorpora um processo de escalonamento de risco e valorização de ativos orientando quanto à sua análise e identificação de riscos e a implantação de controles para minimizá-lo. **A organização pode adotar os padrões da ISO sem necessariamente solicitar a certificação** além disso podemos verificar que a norma não traz as ferramentas a serem adotadas e sim orienta para desenvolver mecanismos de acordo com as suas necessidades do negócio em relação a seus riscos considerando os critérios básicos da SI.

A **documentação do SGSI** deve incluir:

1. declarações documentadas da política e objetivos do SGSI;
2. o escopo do SGSI;
3. procedimentos e controles que apoiam o SGSI;
4. uma descrição da metodologia de análise/avaliação de riscos;
5. o relatório de análise/avaliação de riscos;
6. **o plano de tratamento de riscos;**
7. procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles;
8. registros requeridos por esta Norma; e
9. a Declaração de Aplicabilidade.

**5.1 Liderança e comprometimento**  
**A Alta Direção** deve demostrar sua liderança e **comprometimento**em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a) assegurando que a política de segurança da informação e os objetivos de segurança da informaçao estão estabelecidos e são compatíveis com a direção estratégica da organização;  
b) garantindo a integração dos requisitos do sistema de gestão da segurança da informação dentro dos processos da organização;

c) assegurando que os recursos necessários para o sistema de gestão da segurança da informação estejam disponíveis;  
d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;  
e) assegurando que o sistema de gestão da segurança da informação alcança seus resultados pretendidos;  
f) orientando e apoiando pessoas que contribuam para eficácia do sistema de gestão da segurança da informação;  
**g) promovedo a melhoria contínua; e**  
h) apoiando outros papéis relevantes da gestão para demostrar como sua liderança se aplica às áreas sob sua responsabilidade.

**Requisito de Planejamento da ISO 27001** - **Avaliação de riscos de SI Deverá**

* **Estabelecer e manter critérios de riscos de SI**
* Aceitação de risco
* Desempenho das avaliações dos riscos
* **Assegurar avaliações que produzam resultados** (comparáveis, válidos e consistentes)
* **Identificação dos riscos**
* Riscos associados a perda da CID (confidencialidade, Integridade, Disponibilidade)
* Identificação dos Responsáveis dos riscos
* **Analisar os riscos identificados, avaliando consequências potenciais, se materializados.**
* **Analisar os riscos identificados, avaliando a probabilidade de ocorrência.**
* **Determinar os níveis de risco.**
* **Avaliar os riscos.**
* Comparando os resultados da análise em relação aos critérios que foram estabelecidos (aceitação e desempenho de avaliação).
* Priorizando-os para tratamento

**Seguem os principais controles que foram adicionados no Anexo A da ISO/IEC 27001:2013:**  
  
A.6.1.5 Segurança da Informação no gerenciamento de projetos;  
A.12.6.2 Restrições quanto à instalação de software;  
A.14.2.1 Política de desenvolvimento seguro;  
A.14.2.5 Princípios para projetar sistemas seguros;  
A.14.2.6 **Ambiente seguro para desenvolvimento;**  
A.14.2.8 Testes de segurança do sistema;  
A.15.1.1 Política de Segurança da Informação no relacionamento com os fornecedores.

**16.1.7 Coleta de evidências**

Controle - Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Diretrizes para implementação - Convém que procedimentos internos sejam desenvolvidos e seguidos quando lidando com evidência, para os propósitos de ação legal ou disciplinar.

Em geral, convém que esses procedimentos para evidência forneçam processos de identificação, coleta, aquisição e preservação de evidências, de acordo com diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados.

Convém que os procedimentos levem em conta:

1. cadeia de custódia;
2. segurança da evidência;
3. segurança das pessoas;
4. **papéis e responsabilidades das pessoas envolvidas;**
5. competência do pessoal;
6. documentação;
7. resumo do incidente.

**5 Liderança - 5.3** Autoridades, responsabilidades e papéis organizacionais da segurança da informação sejam atribuídos e comunicados.

**A organização deve conduzir auditorias internas a intervalos planejados para prover informações sobre o quanto o SGSI:**

[...]

c) Planejar, estabelecer, implementar e manter um programa de auditoria (frequência, métodos, responsabilidades, requisitos de planejamento e relatórios) que leve em conta a importância dos processos pertinentes e as **auditorias anteriores**.

**5 Responsabilidades da direção**

5.1 Comprometimento da direção

A Direção deve fornecer evidência do seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI mediante:

1. o estabelecimento da política do SGSI;
2. a garantia de que são estabelecidos os planos e objetivos do SGSI;
3. o estabelecimento de papéis e responsabilidades pela segurança de informação;
4. a comunicação à organização da importância em atender aos objetivos de segurança da informação e a conformidade com a política de segurança de informação, suas responsabilidades perante a lei e a necessidade para melhoria contínua;
5. a provisão de recursos suficientes para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI (ver 5.2.1);
6. a definição de critérios para aceitação de riscos e dos níveis de riscos aceitáveis;
7. a garantia de que as auditorias internas do SGSI sejam realizadas (ver seção 6); e
8. a condução de análises críticas do SGSI pela direção (ver seção 7).

**ISO 27002**

**ISO/IEC 27002** é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação. (Mais detalhada e precisa).

* O controle para seleção de RH deve ser aplicado tanto para funcionários, quanto para fornecedores e outras partes externas.
* A norma sugere que o termo de confidencialidade trate até de obrigações que possam durar após o encerramento da contratação.
* Para aumentar o nível de conscientização, o treinamento deve ter foco não somente no “o quê” e no “como”, mas também no “porquê”.
* Convém que exista um processo disciplinar formal para tomar ações contra funcionários que cometam violações da política.

Existem **três fontes principais de requisitos de segurança da informação.**

1. *Uma fonte é obtida a partir da avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos, e as vulnerabilidades destes e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.*
2. *Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.*
3. *A terceira fonte são os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.*

**5.1.1 Políticas para segurança da informação**

Controle: Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Diretrizes para implementação: Convém que no **mais alto nível** a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Convém que as políticas de segurança da informação contemplem requisitos oriundos de:

a) estratégia do negócio;

b) regulamentações, legislação e contratos;

c) ambiente de ameaça da segurança da informação, atual e futuro.

Convém que a política de segurança da informação contenha declarações relativas a:

a) definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;

b) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;

c) processos para o tratamento dos desvios e exceções.

No **nível mais baixo**, convém que a política de segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos. São exemplos de tais temas de política:

a) controle de acesso (ver 9);

b) classificação e tratamento da informação (ver 8.2);

c) segurança física e do ambiente (ver 11);

d) tópicos orientados aos usuários finais:

1) uso aceitável dos ativos (ver 8.1.3);

2) mesa Limpa e Tela Limpa (ver11.2.9);

3) transferência de informações (ver 13.2.1);

4) dispositivos móveis e trabalho remoto (ver 6.2);

5) restrições sobre o uso e instalação de software (ver 12.6.2);

e) backup (ver 12.3);

f) transferência da informação (ver 13.2);

g) proteção contra malwares (ver 12.2);

h) gerenciamento de vulnerabilidades técnicas (ver 12.6.1);

i) Controles criptográficos (ver 10);

j) segurança nas comunicações (ver 13);

k) proteção e privacidade da informação de identificação pessoal (ver 18.1.4);

l) relacionamento na cadeia de suprimento (ver 15).

**Um exemplo de um esquema de classificação de confidencialidade da informação poderia ser baseado em quatro níveis, a seguir:**

1. quando sua divulgação não causa nenhum dano;
2. quando a divulgação causa constrangimento menor ou inconveniência operacional menor;
3. quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;
4. quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

**SEGURANÇA EM RECURSOS HUMANOS:**

* **Antes da Contratação: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidades com os papéis para os quais eles foram selecionados;**
* **Durante a Contratação: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação;**
* **Encerramento e mudança da contratação: Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.**

**6 Organização da segurança da informação**

6.1.2 Segregação de funções

Controle - Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização”.

**5 Políticas de segurança da informação**

5.1 Orientação da direção para segurança da informação

Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

5.1.1 Políticas para segurança da informação – Controle - Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Diretrizes para implementação - Convém que, no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação.

Convém que as políticas de segurança da informação contemplem requisitos oriundos de:

* estratégia do negócio;
* **regulamentações, legislação e contratos;**
* ambiente de ameaça da segurança da informação, atual e futuro.

**8.2.1 Classificação da informação**

**[...]**

**Diretrizes para implementação**

[...]

Convém que os proprietários de ativos de informação sejam responsáveis por sua classificação.

**8.2.2 Rótulos e tratamento da informação**

*Controle* :Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

Diretrizes para implementação:

**O procedimento pode definir uma situação onde a rotulação é omitida**, por exemplo, rotulação de informação não confidencial, para reduzir a carga de trabalho. Convém que os funcionários e partes externas estejam conscientes do procedimento de classificação da informação.

**8.2 Classificação da informação**

**8.2.1 Classificação da informação**

Controle - Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

**Acesso**

**9.1.1 - Política de controle de acesso** - Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de SI e dos negócios.   
  
Diretrizes para implementação  
  
Convém que os proprietários dos ativos determinem regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados.

* Considerar legislação pertinente e qualquer obrigação contratual.
* Definir requisitos para autorização formal de pedidos de acesso, análise crítica periódica de direitos e remoção de direitos.
* Definir regras para o acesso privilegiado.

Obs.: “Tudo é proibido a menos que expressamente permitido.“ Obs.: Abordagem da necessidade “de conhecer” e “de usar”.

**9.1.2 - Acesso às redes e aos serviços de rede** - Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

* Procedimentos para autorizar acesso a redes e a serviços de redes.
* Controles para proteger o acesso a conexões e a serviços de redes.
* Requisitos de autenticação do usuário para acessar serviços de rede e monitoramento do uso dos serviços de rede.

**Trabalho remoto**  
Controle  
Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para **proteger**as informações acessadas, **processadas**ou armazenadas em locais de**trabalho remoto.**

**11 Segurança física e do ambiente**

**11.1.2 Controles de entrada física**

Diretrizes para implementação:

(...)

b) convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados, por exemplo, mecanismos de autenticação de **dois fatores**, como, cartões de controle de acesso e PIN (personal identification number);

(...) ISO 27002 2013, pág 39.

**8.1.2 Proprietário dos ativos**

Controle - Convém que os ativos mantidos no inventário tenham um proprietário.

**Informações adicionais**

O proprietário identificado pode ser um indivíduo ou uma entidade que aprovou a responsabilidade pela gestão, para controlar todo o ciclo de vida de um ativo. O proprietário identificado não tem necessariamente quaisquer direitos de propriedade sobre o ativo.

**16 Gestão de incidentes de segurança da informação**

**16.1.2 Notificação de eventos de segurança da informação**

Controle

Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

Situações a serem consideradas para **notificar um evento** de segurança da informação incluem:

1. controle de segurança ineficaz;
2. violação da disponibilidade, confidencialidade e integridade da informação;
3. **erros humanos;**
4. não-conformidade com políticas ou diretrizes;
5. violações de procedimentos de segurança física;
6. mudanças descontroladas de sistemas;
7. mau funcionamento de software ou hardware;
8. violação de acesso.

**16 Gestão de incidentes de segurança da informação**

**16.1 Gestão de incidentes de segurança da informação e melhorias**

Diretrizes para implementação

Convém que as seguintes diretrizes para o gerenciamento de responsabilidades e procedimentos com relação à gestão de incidentes de segurança da informação sejam consideradas:

b) procedimentos estabelecidos assegurem que:

2) um ponto de contato para notificação e detecção de incidentes de segurança está implementado;

**6 Organização da Segurança da Informação**

**6.1 Organização interna**

**6.1.5 Segurança da informação no gerenciamento de projetos**

Diretrizes para implementação

(...)

Convém que as questões de segurança da informação sejam consideradas e analisadas criticamente a intervalos planejados, em todos os projetos. **Convém que as responsabilidades pela segurança da informação sejam definidas e alocadas para papéis específicos definidos dos métodos de gerenciamento de projeto.**

O controle de segurança física e do ambiente se divide em duas "vertentes":

.

**11 SEGURANÇA FÍSICA E DO AMBIENTE:**

*11.1 Áreas seguras*

*Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.*

*.*

*11.2 Equipamentos*

*Objetivo:****Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização****.*

**9.1.2 Acesso às redes e aos serviços de rede**

Controle - Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

**Descarte de mídias:**

* Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

**Transferência física de mídias:**

* Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

**8.3.1 Gerenciamento de mídias removíveis**  
  
**Controle -** Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

**Diretrizes para implementação**  
Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas:  
  
a)quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;

**Capítulo 7 Apoio**

7.3 Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

* política de segurança da informação;
* suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e
* implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

**16.1.5 Resposta aos incidentes de segurança da informação**  
  
Controle - Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados. Informações adicionais  
  
**O primeiro objetivo de resposta a incidente é “voltar ao nível de segurança normal” e então iniciar a recuperação necessária.**

**2.2.1 Controles contra códigos maliciosos**

Informações adicionais - **A utilização de dois ou mais tipos de software de controle contra códigos maliciosos de diferentes fornecedores e tecnologias no ambiente de processamento da informação pode aumentar a eficácia na proteção contra códigos maliciosos.”.**

**6 Organização da segurança da informação  
  
6.1 Organização interna  
  
6.1.4 Contato com grupos especiais**

a) ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre segurança da informação;  
  
b) assegurar que o entendimento do ambiente de segurança da informação está atual e completo;  
  
c) receber previamente advertências de alertas, aconselhamentos e correções relativos a ataques e vulnerabilidades;  
  
d) conseguir acesso à consultoria especializada em segurança da informação;  
  
**e) compartilhar e trocar informações sobre novas tecnologias, produtos, ameaças ou vulnerabilidades;**  
  
f) prover relacionamentos adequados quando tratar com incidentes de segurança da informação.

**ISO 27005**

Segundo a ISO 27005:2011," 7.1 Considerações Gerais. É essencial determinar o **propósito da gestão de riscos de segurança da informação**, pois ele afeta o processo em geral e a definição do contexto em particular. **Esse propósito pode ser:**

Suporte a um SGSI.  
Conformidade legal e evidência da devida diligência (“due diligence”).  
Preparação de um plano de continuidade de negócios.  
**Preparação de um plano de resposta a incidentes.**

Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

**O processo de gestão de riscos de segurança da informação consiste na:**

**definição do contexto** (Seção 7)  
**processo de avaliação de riscos** (Seção 8)  
**tratamento do risco** (Seção 9)  
**aceitação do risco** (Seção 10)  
**comunicação e consulta do risco** (Seção 11) e  
**monitoramento e análise crítica de riscos** (Seção 12).

**Ciclo de vida da gestão de risco**

* **Etapa 1 Identifique o risco:** Você e sua equipe descobrem, reconhecem e descrevem riscos que podem afetar seu projeto ou seus resultados. Existem várias técnicas que você pode usar para encontrar os riscos do projeto. Durante esta etapa, você começa a preparar seu Registro de riscos do projeto.
* **Etapa 2 Analise o risco:** Uma vez identificados os riscos, você determina a probabilidade e a consequência de cada risco. Você desenvolve uma compreensão da natureza do risco e seu potencial para afetar as metas e objetivos do projeto. Essas informações também são inseridas no seu Registro de riscos do projeto.
* **Etapa 3 Avalie ou classifique o risco:** Você avalia ou classifica o risco determinando a magnitude do risco, que é a combinação de probabilidade e consequência. Você toma decisões sobre se o risco é aceitável ou se é sério o suficiente para garantir o tratamento. Essas classificações de risco também são adicionadas ao seu Registro de riscos do projeto.
* **Etapa 4 Trate o risco**: Isso também é chamado de Planejamento de respostas a riscos. Durante esta etapa, você avalia seus riscos mais bem classificados e define um plano para tratar ou modificar esses riscos para atingir níveis de risco aceitáveis. Como você pode minimizar a probabilidade dos riscos negativos e aumentar as oportunidades? Você cria estratégias de mitigação de risco, planos preventivos e planos de contingência nesta etapa. E você adiciona as medidas de tratamento de risco para os riscos mais altos ou mais graves para o seu registro de riscos do projeto.
* **Etapa 5 Monitore e analise o risco:** Este é o passo em que você pega o Registro de Risco do Projeto e o utiliza para monitorar, rastrear e revisar os riscos.

Opções do tratamento do risco: **MERC**

* **Modificar o risco -** Convém que o nível de risco seja gerenciado através da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.
* **Reter o risco -** Convém que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos. Não há necessidade de se implementar controles adicionais e pode haver a retenção do risco.
* **Evitar o Risco -** Convém que a atividade ou condição que dá origem a um determinado risco seja evitada. Decidir que o risco seja evitado completamente, seja através da eliminação de uma atividade planejada ou existente, seja através de mudanças nas condições em que a operação da atividade ocorre.
* **Compartilhar o Risco -** Convém que um determinado risco seja compartilhado com outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos. ISO 27005, pág. 32

**As quatro opções para o tratamento do risco não são mutuamente exclusivas.** Às vezes, a organização pode beneficiar-se substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais.

"8.3 Análise de riscos

8.3.1 Metodologias de análise de riscos

Na prática, a análise qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Depois, poderá ser necessário efetuar uma análise quantitativa ou mais específica, nos grandes riscos. Isso ocorre porque normalmente é menos complexo e menos oneroso realizar análises qualitativas do que quantitativas.

...

A análise qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo, Pequena, Média e Grande) e a probabilidade dessas consequências ocorrerem. Uma vantagem da análise qualitativa é sua facilidade de compreensão por todas as pessoas envolvidas enquanto que uma desvantagem é a dependência à escolha subjetiva da escala.

...

A análise quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização."

"**Uma ameaça pode surgir de dentro ou de fora da organização.** Convém que as ameaças sejam identificadas genericamente e por classe (por exemplo, ações não autorizadas, danos físicos, falhas técnicas) e, quando apropriado, ameaças especificas identificadas dentro das classes genéricas. Isso significa que, nenhuma ameaça é ignorada, incluindo as não previstas, mas que o volume de trabalho exigido é limitado."

Ademais, a identificação de ameaças recebe como entrada "informações sobre ameaças obtidas a partir da análise crítica de incidentes, dos responsáveis pelos ativos, de usuários e de outras fontes, **incluindo catálogos externos de ameaças.**”.

"Convém que um responsável seja identificado para cada ativo, a fim de oficializar sua responsabilidade e garantir a possibilidade da respectiva prestação de contas. **O responsável pelo ativo pode não ter direitos de propriedade sobre o mesmo**, mas tem responsabilidade sobre sua produção, desenvolvimento, manutenção, utilização e segurança, conforme apropriado. O responsável pelo ativo é frequentemente a pessoa mais adequada para determinar o valor do mesmo para a organização."

**A ISO 27005 adota o ciclo PDCA:**

-Em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase "planejar"(PLAN).

-Na fase "executar" (DO) do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco.

-Na fase “verificar” (CHECK) do SGSI, os gestores determinarão a necessidade de revisão das avaliações e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias.

-Na fase “agir” (ACT), as ações necessárias são executadas, **incluindo a reaplicação do processo de gestão de riscos de segurança da informação.**

Manter e melhorar o processo de gestão de riscos da segurança da informação **está alinhado com a fase agir** do SGSI. Trata-se de uma ação corretiva.

De acordo com a norma ISO 27005, **exemplos do escopo da gestão de riscos podem ser: uma aplicação de TI**, a infraestrutura de TI, **um processo de negócios** ou uma parte definida da organização.

**Planejar**

* Definição do contexto
* Processo de avaliação de riscos
* Definição do plano de tratamento do risco
* Aceitação do risco

**Executar**

* Implementação do plano de tratamento do risco

**Verificar**

* Monitoramento continuo e análise crítica de riscos

**Agir**

* Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

**Identificação de ativos na organização**

**Primários**

* Informação
* Processos e Atividades de negócios

**Suporte e Infraestrutura**

* Hardware
* Software
* Rede
* Recursos Humanos
* Instalações Físicas
* Estruturas Organizacionais

**As principais etapas do processo de gestão de riscos são:**

* Definição do Contexto
* Processos de Avaliação de Riscos
* Tratamentos dos Riscos
* Aceitação dos Riscos

E ainda os processos paralelos de "Comunicação e Consulta do Risco" e "Monitoramento e Análise Crítica do Risco"

**Risco residual:** o risco remanescente após o tratamento do risco inicialmente observado.

**NOTA 1 -** O risco residual pode conter riscos não identificados.  
**NOTA 2** - O risco residual também pode ser conhecido como "risco retido".

**Tratamento do risco:**

* **Modificação do risco:**Ações tomadas para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.
* **Evitar o risco:**Decisão de não se envolver ou agir de forma a mitigar uma situação de risco.
* **Retenção do risco:**Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco.
* **Compartilhamento do risco:**Compartilhamento com outra entidade do ônus da perda ou do benefício do ganho associado a um risco.

**11 Segurança física e do ambiente**

**11.1 Áreas seguras -** Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.

**11.1.1 Perímetro de segurança física -** Controle: Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.

**11.2.9 Política de mesa limpa e tela limpa -** Controle: Convém que seja adotada uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

Diretrizes para implementação: Convém que uma política de mesa limpa e tela protegida leve em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da organização. Convém que as seguintes diretrizes sejam consideradas:

a) convém que as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório estiver desocupado;

b) convém que os computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;

c) convém que sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, scanners, máquinas fotográficas digitais);

d) convém que os documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

Informações adicionais

Uma política de mesa limpa e tela protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

**8 Processo de avaliação de riscos de segurança da informação**  
  
**8.1 Descrição geral do processo de avaliação de riscos de segurança da informação**

**Entrada:** **Critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos de segurança da informação que se está definindo.**  
  
**Ação:**Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

**Diretrizes para implementação: -** Um risco é a combinação das consequências advindas da ocorrência de um evento indesejado e da probabilidade da ocorrência do mesmo. O processo de avaliação de riscos quantifica ou descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos. O processo de avaliação de riscos consiste nas seguintes atividades: Identificação de riscos (Seção 8.2); Análise de riscos (Seção 8.3);   
Avaliação de riscos (Seção 8.4);

**8.3.1 Metodologias de análise de riscos**

A análise qualitativa pode ser utilizada:

* Como uma verificação inicial a fim de identificar riscos que exigirão uma análise mais detalhada;
* Quando esse tipo de análise é suficiente para a tomada de decisões;
* Quando os dados numéricos ou recursos são insuficientes para uma análise quantitativa;

**Alinhamento do processo do SGSI e do processo de gestão de riscos de segurança da informação**

**Processo do SGSI**  -  Processo de gestão de riscos de segurança da informação

* **Planejar**-  Definição do contexto; Processo de avaliação de riscos; Definição do plano de tratamento do risco; Aceitação do risco;
* **Executar**-  Implementação do plano de tratamento do risco;
* **Verificar**-  Monitoramento contínuo e análise crítica de riscos
* **Agir**-  Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

[**Análise de Vulnerabilidade e Gestão de Riscos**](https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-seguranca-da-informacao/analise-de-vulnerabilidade-e-gestao-de-riscos)

Risco é a medida da exposição a qual o sistema computacional está sujeito. Depende de a probabilidade de uma ameaça atacar o sistema e do impacto resultante desse ataque. Sêmola (2003, p. 50), diz que risco é a **“probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios”**. **Risco *é o efeito da incerteza nos objetivos.***

Primeiramente, o contexto é estabelecido. Em seguida, os riscos são **IDENTIFICADOS**, analisados e **AVALIADOS**. Se estas etapas fornecem informações suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode prosseguir.

**ISO 31000 - Processo**

* Comunicação e consulta
* Estabelecimento do contexto (externo, interno, contexto de processo, definição de critérios de risco).
* Processo de avaliação dos riscos (identificação, análise, avaliação)
* Tratamento dos riscos (seleção de opções, preparação e implementação de planos de tratamento).
* Monitoramento e Análise crítica
* Registro do processo

A **análise de riscos** inclui:

● Identificação dos riscos

● Estimativas dos riscos

● Avaliação dos riscos

O risco de auditoria é uma função dos riscos de distorção relevante e do risco de detecção, a seguir discriminados:

* **Risco de detecção:** é o risco de que os procedimentos executados pelo auditor não detectem uma distorção potencialmente relevante, individualmente ou em conjunto com outras distorções.
* **Risco de distorção relevante:**é o risco de que as demonstrações contábeis contenham distorção relevante antes da auditoria. Consiste em dois componentes, o risco inerente e o risco de controle:
* **Risco inerente:** é a suscetibilidade de uma afirmação a respeito de uma transação, saldo contábil ou divulgação, a uma distorção que possa ser relevante, individualmente ou em conjunto com outras distorções, antes de se considerar qualquer controle preexistente;
* **Risco de controle:** é o risco de que uma distorção não seja prevenida, detectada e corrigida tempestivamente pelo controle interno da entidade.

**6.4.4 Avaliação de riscos**

O propósito da **avaliação de riscos**é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

* Fazer mais nada;
* Considerar as opções de tratamento de riscos;
* Realizar análises adicionais para melhor compreender o risco;
* Manter os controles existentes.
* Reconsiderar os objetivos;

ISO 31000-2018