\*\* VERSÃO DE DEMONSTRAÇÃO \*\*

Obrigado por baixar a versão de visualização gratuita do Kit de documentação ISO 27001.

[logotipo da organização]

[nome da organização]

**METODOLOGIA DE AVALIAÇÃO E TRATAMENTO DE RISCOS**

|  |  |
| --- | --- |
| Código: |  |
| Versão: |  |
| Data da versão: |  |
| Criado por: |  |
| Aprovado por: |  |
| Nível de confidencialidade: |  |

**Histórico de alterações**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Criado por** | **Descrição da alteração** |
|  | 0.1 | Advisera | Esboço básico do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc152755418)

[2. Documentos de referência 3](#_Toc152755419)

[3. Metodologia de avaliação e tratamento de riscos 3](#_Toc152755420)

[3.1. Avaliação de riscos 3](#_Toc152755421)

[3.1.1. O processo 3](#_Toc152755422)

[3.1.2. Ativos, vulnerabilidades e ameaças 3](#_Toc152755423)

[3.1.3. Determinar os proprietários do risco 4](#_Toc152755424)

[3.1.4. Consequências e probabilidades 4](#_Toc152755425)

[3.2. Critérios de aceitação de riscos 4](#_Toc152755426)

[3.3. Tratamento de riscos 4](#_Toc152755427)

[3.4. Análises periódicas da avaliação e do tratamento de riscos 5](#_Toc152755428)

[3.5. Declaração de aplicabilidade e Plano de tratamento de riscos 5](#_Toc152755429)

[3.6. Geração de relatórios 5](#_Toc152755430)

[4. Gestão de registros mantidos de acordo com este documento 6](#_Toc152755431)

[5. Validade e gestão de documentos 7](#_Toc152755432)

[6. Anexos 7](#_Toc152755433)

# Finalidade, escopo e usuários

A finalidade deste documento é definir a metodologia de avaliação e tratamento de riscos à informação na [nome da organização] e definir o nível aceitável de riscos de acordo com a norma ISO/IEC 27001.

A avaliação de riscos aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os ativos que são usados na organização ou que podem ter um impacto sobre a segurança da informação no SGSI.

Os usuários deste documento são funcionários da [nome da organização] que fazem parte da avaliação e do tratamento de riscos.

# Documentos de referência

* Norma ISO/IEC 27001, cláusulas 6.1.2, 6.1.3, 8.2 e 8.3
* Política de segurança da informação
* Lista de requisitos legais, regulatórios, contratuais e outros
* Política de segurança do fornecedor
* Declaração de aplicabilidade

# Metodologia de avaliação e tratamento de riscos

## Avaliação de riscos

### O processo

A avaliação dos riscos é implementada por meio da Tabela de avaliação de riscos. O processo de avaliação de riscos é coordenado pelo [cargo], e identificação de ameaças e vulnerabilidades é realizada pelos proprietários do ativo, enquanto a avaliação das conseqüências e probabilidade é realizada pelos proprietários do risco. [Cargo] é responsável por incluir os dados sobre ameaças, vulnerabilidades, consequências e probabilidades na Tabela de avaliação de riscos.

### Ativos, vulnerabilidades e ameaças

A primeira etapa da avaliação de riscos é a identificação de todos os ativos no escopo do SGSI pelos representantes de cada área no escopo do SGSI, isso é, de identificar todos os ativos que podem afetar a confidencialidade, integridade e disponibilidade das informações na organização. Os ativos podem incluir documentos em papel ou formato eletrônico, aplicativos e bancos de dados, pessoas, equipamentos de TI, infraestrutura e serviços externos e serviços contratados. Ao identificar os ativos, também é preciso identificar seus "proprietários", as pessoas ou a unidade organizacional responsável para cada ativo.

A próxima etapa é a identificação, pelos donos de ativos, de todas as ameaças e vulnerabilidades associadas a cada ativo. As ameaças e vulnerabilidades são identificadas por meio do catálogo incluído na Tabela de avaliação de riscos. Cada ativo pode estar associado a diversas ameaças e cada ameaça pode estar associada a diversas vulnerabilidades.

### Determinar os proprietários do risco

Para cada risco, um proprietário do risco precisa ser identificado – pessoa ou unidade organizacional responsável por cada risco – esta pessoa pode ou não ser a mesma que o proprietário do ativo.

### Consequências e probabilidades

Após a identificação dos proprietários do risco, é necessário avaliar as conseqüências para cada combinação de ameaças e vulnerabilidades para a um determinado ativo se tal risco se materialize:

|  |  |  |
| --- | --- | --- |
| Baixa consequência | 0 | A perda da confidencialidade, disponibilidade ou integridade não afeta o fluxo de caixa, as obrigações legais ou contratuais ou sua reputação. |
| Consequência moderada | 1 | A perda da confidencialidade, disponibilidade ou integridade gera custos ou possui um impacto moderado ou baixo sobre as obrigações legais ou contratuais ou sobre a reputação da organização. |
| Alta consequência | 2 | A perda da confidencialidade, disponibilidade ou integridade tem impacto considerável e imediato sobre o fluxo de caixa da organização, as obrigações legais ou contratuais ou sua reputação. |

Após a avaliação das consequências, é necessário avaliar a probabilidade da ocorrência do risco, ou seja, a probabilidade de que uma ameaça irá se aproveitar da vulnerabilidade do ativo em questão:

|  |  |  |
| --- | --- | --- |
| Baixa probabilidade | 0 | Os controles de segurança existentes são fortes e até agora forneceram o nível de proteção adequado. Nenhum novo incidente é esperado no futuro. |
| Probabilidade moderada | 1 | Os controles de segurança existentes são moderados e na maioria das situações forneceram o nível de proteção adequado. Novos incidentes são possíveis, mas com pouca probabilidade. |
| Alta probabilidade | 2 | Os controles de segurança existentes são poucos ou ineficazes. Há grandes probabilidades de que esses incidentes ocorram no futuro. |

...

\*\* FIM DA DEMONSTRAÇÃO \*\*

Se você decidiu que o Kit de Documentação ISO 27001 é a escolha certa para sua empresa, consulte a tabela abaixo para escolher o kit com o nível de suporte especializado necessário.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Kit de documentos com suporte especializado** | **Kit de documentos com suporte extendido** | **Kit de documentos power** |
|  | **US $897** | **US $1397** | **US $2397** |
| **45 modelos de documentos em conformidade com a ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Acesso a tutoriais em vídeo (em Inglês)** | **🗸** | **🗸** | **🗸** |
| **Em breve: atualização gratuita do kit de documentação para a nova revisão da ISO 27001 2022** | **🗸** | **🗸** | **🗸** |
| **ISO 27001 Gap Analysis Tool** | **🗸** | **🗸** | **🗸** |
| **Suporte por e-mail** | 10 perguntas por mês | Ilimitado | Ilimitado |
| **Suporte individual com um especialista em ISO 27001** | 1 hora | 5 horas | 15 horas |
| **Revisão por um especialista (documentos preenchidos)** | 1 documento | 5 documentos | 15 documentos |
| **Treinamento de conscientização sobre segurança (em Inglês)** | **X** | 20 usuários | 50 usuários |
| **Verificação pré-auditoria** | **X** | **🗸** | **🗸** |
|  | [**COMPRE AGORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718471&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=pt-br?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-expert-support&utm_content=lang-pt-br) | [**COMPRE AGORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718470&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=pt-br?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-extended-support&utm_content=lang-pt-br) | [**COMPRE AGORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718469&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=pt-br?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-power-support&utm_content=lang-pt-br) |
|  | (clique no link acima usando CTRL+clique) | | |