\*\* VERSÃO DE DEMONSTRAÇÃO \*\*

[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** |
| 01/10/2013 | 0.1 | Dejan Kosutic | Esboço básico do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc368903472)

[2. Documentos de referência 3](#_Toc368903473)

[3. Metodologia de avaliação e tratamento de riscos 3](#_Toc368903474)

[3.1. Avaliação de riscos 3](#_Toc368903475)

[3.1.1. O processo 3](#_Toc368903476)

[3.1.2. Ativos, vulnerabilidades e ameaças 3](#_Toc368903477)

[3.1.3. Determinar os proprietários do risco 3](#_Toc368903478)

[3.1.4. Consequências e probabilidades 4](#_Toc368903479)

[3.2. Critérios de aceitação de riscos 4](#_Toc368903480)

[3.3. Tratamento do risco 4](#_Toc368903481)

[3.4. Análises periódicas da avaliação e do tratamento de riscos 5](#_Toc368903482)

[3.5. Declaração de Aplicabilidade e Plano de tratamento do risco 5](#_Toc368903483)

[3.6. Geração de relatórios 5](#_Toc368903484)

[4. Gestão de registros mantidos de acordo com este documento 6](#_Toc368903485)

[5. Validade e gestão de documentos 7](#_Toc368903486)

[6. Anexos 7](#_Toc368903487)

# 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 do sistema de gestão da segurança da informação
* 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 vulnerabilidade é realizada pelos proprietários do ativo, enquanto a avaliação das conseqüências e probabilidade é realizada pelos proprietários do risco.

### Ativos, vulnerabilidades e ameaças

A primeira etapa da avaliação de riscos é a identificação de todos os ativos no escopo do SGSI, isso é, de 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, 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.

\*\* FIM DA DEMONSTRAÇÃO \*\*

Clique aqui para baixar a versão completa deste documento: <http://www.iso27001standard.com/pt/documentacao/Metodologia-de-avaliacao-e-tratamento-de-riscos>