\*\* VERSÃO DE DEMONSTRAÇÃO \*\*

[logotipo da organização]

[nome da organização]

**DECLARAÇÃO DE APLICABILIDADE**

|  |  |
| --- | --- |
| 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](#_Toc368895801)

[2. Documentos de referência 3](#_Toc368895802)

[3. Aplicabilidade dos controles 3](#_Toc368895803)

[4. Declaração de aceitação de riscos residuais 20](#_Toc368895804)

[5. Validade e gestão de documentos 20](#_Toc368895806)

# Finalidade, escopo e usuários

A finalidade deste documento é definir quais controles são adequados para implementação na [nome da organização], quais são os objetivos desses controles e como eles são implementados, além de aprovar riscos residuais e aprovar formalmente a implementação desses controles.

Este documento inclui todos os controles relacionados no Anexo A da norma ISO 27001. Os controles são aplicáveis a todo o escopo do Sistema de gestão da segurança da informação (SGSI).

Os usuários deste documentos são funcionários da [nome da organização] que trabalham no objetivo da SGSI.

# Documentos de referência

* Norma ISO/IEC 27001, cláusula 6.1.3.d)
* Política do sistema de gestão da segurança da informação
* Metodologia de avaliação e tratamento de riscos
* Relatório de avaliação de riscos e de tratamento do risco

# Aplicabilidade dos controles

Os seguintes controles do Anexo A da ISO 27001 são aplicáveis:

| ID | Controles de acordo com a norma ISO/IEC 27001 | Aplicabilidade (SIM/NÃO) | Justificativa para a seleção/não seleção | Objetivos do controle | Método de implementação | Status |
| --- | --- | --- | --- | --- | --- | --- |
| A.5 | Política da segurança da informação |  |  |  |  |  |
| A.5.1 | Direção gerencial para a segurança da informação |  |  |  |  |  |
| A.5.1.1 | Políticas para a segurança  da informação |  |  |  | Todas as políticas referidas abaixo nesta coluna |  |
| A.5.1.2 | Revisão das políticas  para a segurança  da informação |  |  |  | Cada política tem um proprietário designado, que deve rever o documento nos intervalos planejados |  |
| A.6 | Organização da segurança da informação |  |  |  |  |  |
| A.6.1 | Organização interna |  |  |  |  |  |
| A.6.1.1 | Funções e responsabilidades da  segurança da informação |  |  |  | As responsabilidades para a segurança da informação são listadas em diversos documentos do SGSI. Se necessário, o [nome do cargo] define outras responsabilidades |  |
| A.6.1.2 | Segregação de funções |  |  |  | Qualquer atividade que inclua informações sensíveis é aprovada por uma pessoa e implementada por outra |  |
| A.6.1.3 | Contato com autoridades |  |  |  | [Estratégia de continuidade de negócios], [Plano de resposta aos incidentes] |  |
| A.6.1.4 | Contato com grupos  de interesse especial |  |  |  | O [nome do cargo] é responsável por monitorar [liste os nome de grupos de interesse e de fóruns de segurança] |  |
| A.6.1.5 | Segurança da informação  na gerência de projeto |  |  |  | O Gerente de Projeto deve incluir as regras de segurança da informação aplicáveis em cada projeto |  |
| A.6.2 | Dispositivo móvel e trabalho remoto |  |  |  |  |  |
| A.6.2.1 | Política de dispositivo móvel |  |  |  | [Política de uso aceitável] / [Política de dispositivo móvel e trabalho remoto], [Traga sua própria política de dispositivo (BYOD)] |  |
| A.6.2.2 | Trabalho remoto |  |  |  | [Política de uso aceitável de ativos] / [Dispositivo móvel e trabalho remoto] |  |

\*\* FIM DA DEMONSTRAÇÃO \*\*

# Clique aqui para baixar a versão completa deste documento: <http://www.iso27001standard.com/pt/documentacao/Declaracao-de-aplicabilidade>