\*\* VERSÃO DE DEMONSTRAÇÃO \*\*

Obrigado por baixar a versão de visualização gratuita do Kit de Avaliação de Riscos da ISO 27001/ISO 22301.

[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** |
|  | 0.1 | Advisera | Esboço básico do documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sumário**

[1. Finalidade, escopo e usuários 3](#_Toc153270111)

[2. Documentos de referência 3](#_Toc153270112)

[3. Aplicabilidade dos controles 3](#_Toc153270113)

[4. Aceitação de riscos residuais 19](#_Toc153270114)

[5. Validade e gestão de documentos 20](#_Toc153270115)

# 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 documento 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 de segurança da informação
* Metodologia de avaliação e tratamento de riscos
* Relatório de avaliação e tratamento de riscos

# 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 | ... | ... | ... |
| --- | --- | --- | --- | --- | --- | --- |
| A.5.1 | Políticas de segurança da informação |  |  |  | ... |  |
| A.5.2 | Papéis e responsabilidades pela segurança da informação |  |  |  | ... |  |
| A.5.3 | Segregação de funções |  |  |  | Qualquer atividade que inclua informações sensíveis é aprovada por uma pessoa e implementada por outra. |  |
| A.5.4 | Responsabilidades da direção |  |  |  | A direção requer ativamente que todas as regras do SGSI sejam implementadas por todos os funcionários, fornecedores e parceiros de terceirização. |  |
| A.5.5 | Contato com autoridades |  |  |  | O [cargo] é responsável pelo contato com as autoridades apropriadas (por exemplo, polícia, corpo de bombeiros, etc.)  [Estratégia de continuidade de negócios], [Plano de resposta a incidentes] |  |
| A.5.6 | Contato com grupos de interesse especial |  |  |  | O [cargo] é responsável por monitorar [liste os nomes de grupos de interesse e de fóruns de segurança]. |  |
| A.5.7 | Inteligência de ameaças |  |  |  | [Política de segurança do fornecedor], [Procedimento de gestão de incidentes], [Procedimentos de segurança para o departamento de TI] |  |

...

# Aceitação de riscos residuais

Como nem todos os riscos podem ser reduzidos no processo de gestão de riscos, todos os riscos residuais descritos aqui são aceitos:

1. todos os riscos com o valor 0, 1 ou 2
2. os riscos que não podem ser reduzidos aos níveis mencionados acima, após a aplicação dos controles, de acordo com a tabela a seguir:

[Preencha a tabela com os dados sobre todos os riscos individuais que não são aceitáveis; use a Tabela de tratamento de riscos como fonte.]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Num.** | **Nome do ativo** | **Proprietário do ativo** | **...** | **...** | **...** | **...** | **...** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

...

\*\* FIM DA DEMONSTRAÇÃO \*\*

Se você decidiu que o Kit de Avaliação de Riscos da ISO 27001/ISO 22301 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** |
|  | **US $397** | **US $897** |
| **6 modelos de documentos em conformidade com a ISO 27001 e ISO 22301** | **🗸** | **🗸** |
| **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 |
| **Suporte individual com um especialista em ISO 27001 e ISO 22301** | 1 hora | 5 horas |
| **Revisão por um especialista (documentos preenchidos)** | 1 documento | 5 documentos |
| **Verificação pré-auditoria** | **X** | **🗸** |
|  | [**COMPRE AGORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718464&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=pt-br?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-22301-risk-assessment-templates&utm_term=toolkit-with-expert-support&utm_content=lang-pt-br) | [**COMPRE AGORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718465&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=pt-br?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-22301-risk-assessment&utm_term=toolkit-with-extended-support&utm_content=lang-pt-br) |
|  | (clique no link acima usando CTRL+clique) | |