Anexo 3 – Relatório de avaliação e tratamento de riscos

Commented [AES1]: Para aprender como preencher este documento, e ver exemplos reais do que você precisa escrever, veja este vídeo tutorial "How to Write ISO 27001 Risk Assessment Report".

Para acessar o tutorial: Em sua caixa de entrada, encontre o e-mail que você recebeu no momento da compra. Lá, você verá um link e uma senha que lhe permitirá acessar o vídeo tutorial.

Histórico de alterações

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

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é fornecer uma visão geral detalhada do processo e dos documentos usados durante a avaliação de riscos e o tratamento dos riscos disruptivos na [nome da organização] no período [especifique o período].

A avaliação de riscos aplica-se a todo o Sistema de Gestão da Segurança da Informação (SGSI) [Sistema de Gestão da Continuidade de Negócios (SGCN)].

Este documento destina-se à alta direção da [nome da organização], ao [cargo do responsável pela segurança da informação], aos proprietários dos ativos de informações e a todas as pessoas envolvidas no planejamento, na implementação, no monitoramento e na melhoria do SGSI [SGCN].

Commented [AES2]: Inclua o nome da sua organização.

Commented [AES3]: Inclua o nome da sua organização.

Commented [AES4]: Ou "continuidade de negócios".

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 8.2 e 8.3
- Norma ISO 22301 cláusula 8.2.3
- Documento sobre o escopo do SGSI
- Política da segurança da informação
- Política de continuidade de negócios
- Metodologia de avaliação e tratamento de riscos

Commented [AES5]: Você pode encontrar um modelo para este documento na pasta "04_Escopo_do_SGSI" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "10_Documentos_principais_de_continuidade_de_negocios_da_ISO_22301" do Kit de documentação Premium da ISO 27001 e ISO 22301.

3. Processo de avaliação e tratamento de riscos à informação

Todo o processo de avaliação e tratamento de riscos foi desenvolvido de acordo com o documento [illegible]

3.1. Finalidade da gestão de riscos

A finalidade da avaliação de riscos é identificar todos os ativos, suas vulnerabilidades e as ameaças que podem tirar proveito dessas vulnerabilidades, além de avaliar esses parâmetros para estabelecer a importância dos riscos individuais.

[illegible]

3.2. Escopo da avaliação de riscos e do tratamento de riscos

A avaliação e o tratamento de riscos foram desenvolvidos nas [illegible]

Commented [AES8]: Incluir aqui apenas as unidades [illegible]

3.3. Período

A avaliação de riscos foi implementada de [dia/mês/ano] a [dia/mês/ano]. O tratamento de riscos foi implementado de [dia/mês/ano] a [dia/mês/ano]. [illegible]

3.4. Participantes no processo e coleta de informações

O processo de avaliação e tratamento de riscos foi gerenciado por [nome ou cargo] com assistência especializada fornecida por [se houve assistência especializada, forneça o nome da empresa].

[illegible]

Commented [AES9]: Ex.: gerente de continuidade de negócio, [illegible]

Commented [AES10]: Você pode excluir esta parte se [illegible]

Commented [AES11]: Ou descreva outro método se utilizado.

3.5. Breve visão geral da metodologia aplicada

Em poucas palavras, o processo foi conduzido da seguinte forma:

- todos os ativos de informações foram identificados, assim como seus proprietários
- as ameaças foram identificadas para cada ativo e as vulnerabilidades correspondentes foram identificadas para cada ameaça
- [illegible]
- [illegible]
- a probabilidade de ocorrência de riscos, isto é, de que a ameaça aproveite a vulnerabilidade, que foi avaliada com valores entre 0 e 2
- o nível do risco foi calculado com a adição das consequências e da probabilidade
- [illegible]
- [illegible]
- depois da aplicação dos controles, os riscos residuais foram avaliados

Commented [AES12]: Excluir este texto se apenas os controles [illegible]

3.6. Visão geral dos documentos usados durante o processo de avaliação e tratamento de riscos

Os seguintes documentos foram usados ou elaborados durante a implementação da avaliação e do tratamento dos riscos:

- Tabela de avaliação de riscos (Anexo 1) – para cada combinação de ativos, vulnerabilidade e ameaças mostra os calores para a consequência e probabilidade, e calcula o risco
- [illegible]

4. Validade e gestão de documentos

Este documento é válido a partir de [data]. [illegible]

Commented [AES13]: Ex.: gerente de continuidade de [illegible]

5. Anexos

- Anexo 1 – Tabela de avaliação de riscos

- Anexo 2 – Tabela de tratamento de riscos

[cargo]
[nome]

[assinatura]

Commented [AES14]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.