[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:	

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

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.

Commented [AES2]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

Commented [AES3]: Para aprender como escrever a metodologia, leia estes artigos:

- Avaliação e tratamento de riscos segundo a ISO 27001 – 6 etapas básicas https://advisera.com/27001academy/pt-br/knowledgebase/avaliacao-e-tratamento-de-riscos-segundo-a-iso-27001-6-etapas-basicas/
- Como escrever metodologia de avaliação de riscos para a ISO 2700 https://advisera.com/27001academy/pt-br/knowledgebase/como-escrever-metodologia-de-avaliacao-de-riscos-para-a-iso-27001/

Commented [AES4]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

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 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.

Commented [AES5]: Inclua o nome da sua organização.

Commented [AES6]: Ou escreva "norma ISO 22301" se você estiver implementando somente a continuidade de negócios.

Commented [AES7]: Ou escreva "Sistema de Gestão da Continuidade de Negócios (SGCN)" se você estiver implementando somente a continuidade de negócios.

Commented [AES8]: Ou escreva "SGCN" se você estiver implementando somente a continuidade de negócios.

Commented [AES9]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 6.1.2, 6.1.3, 8.2 e 8.3
- Norma ISO 22301, cláusulas 8.2.1 e 8.2.3
- Política de segurança da informação
- Lista de requisitos legais, regulatórios, contratuais e outros
- Política de segurança do fornecedor
- Declaração de aplicabilidade

Commented [AES10]: Exclua isto se você estiver implementando somente a norma ISO 22301.

Commented [AES11]: Exclua isto se você estiver implementando somente a norma ISO 27001.

Commented [AES12]: Exclua isto se você estiver implementando somente a norma ISO 22301.

Commented [AES13]: Você pode encontrar um modelo para este documento na pasta "03_Identificacao_de_requisitos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES14]: Exclua se não deseja usar esta Política.

Commented [AES15]: Exclua isto se você estiver implementando somente a norma ISO 22301.

3. Metodologia de avaliação e tratamento de riscos

Commented [AES16]: Esta Metodologia deve ser corrigia se

3.1. Avaliação de riscos

3.1.1. 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.

Commented [AES17]: Para simplificar o processo, você pode definir que o proprietário do ativo para cada risco também seja o proprietário do risco.

3.1.2. 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.

Commented [AES18]: Ou "SGCN".

Commented [AES19]: Ou "SGCN".

Commented [AES20]: Adicione os demais tipos de ativos que

A próxima etapa é a identificação, para cada item de ativo, 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.

3.1.3. Determinar os proprietários do risco

Para cada risco, um proprietário do risco precisa ser identificado – pessoa ou unidade organizacional responsável por cada risco – [illegible]

Commented [AES21]: Para simplificar o processo, você pode [illegible]

3.1.4. 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.
[illegible]	1	[illegible]
[illegible]	2	[illegible]

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.
[illegible]	1	[illegible]
[illegible]	2	[illegible]

Ao inserir os valores da consequência e da probabilidade na Tabela de avaliação de riscos, o nível do risco é calculado automaticamente com a adição dos dois valores. [illegible]

3.2. Critérios de aceitação de riscos

Os riscos com níveis 0, 1 e 2 são riscos aceitáveis; os riscos com níveis 3 e 4 são riscos inaceitáveis. [illegible]

3.3. Tratamento de riscos

O tratamento de riscos é implementado pela Tabela de tratamento de riscos.

Uma ou mais opções de tratamento devem ser selecionadas para os riscos com níveis 3 e 4:

1. Seleção do controle de segurança ou dos controles da [defina aqui a fonte de controles a serem usados]
2. Transferência dos riscos para terceiros, por exemplo, pela compra de uma apólice de seguro ou um contrato com fornecedores ou parceiros

A seleção das opções é implementada pela Tabela de tratamento de riscos. Geralmente a opção 1 é selecionada (seleção de um ou mais controles de segurança). Quando diversos controles de segurança são selecionados para o risco, mais linhas são inseridas na tabela, logo abaixo da linha que especifica o risco.

No caso da opção 1 (seleção de controles de segurança) ser usada para tratamento de riscos, é necessário avaliar o novo valor da consequência e a probabilidade na Tabela de tratamento de riscos, para poder avaliar a eficácia dos controles planejados.

3.4. Análises periódicas da avaliação e do tratamento de riscos

Os proprietários do risco devem rever os os riscos existentes e atualizar a Tabela de avaliação de riscos e a Tabela de tratamento de riscos de acordo com os riscos identificados recentemente.

3.5. Declaração de aplicabilidade e Plano de tratamento de riscos

O [cargo] precisa documentar o seguinte na Declaração de aplicabilidade: quais controles de segurança do Anexo A da norma ISO/IEC 27001 são aplicáveis e quais não o são, a justificativa de tais decisões e se foram ou não implementados.

Em nome dos proprietários do risco a [alta direção] irá aceitar todos os riscos residuais através da Declaração de aplicabilidade.

3.6. Geração de relatórios

Commented [AES22]: Ex.: gerente de continuidade de

Commented [AES23]: Ex.: controles do Anexo A da norma ISO/IEC 27001, NIST Special Publications, etc.

Commented [AES24]: A seleção dos controles de segurança deve considerar as opções que:
- protejam as atividades comerciais e reduzam a probabilidade de interrupção

Commented [AES25]: Exclua isso se não for usar esta Política.

Commented [AES26]: Este novo valor é denominado "Risco Residual".

Commented [AES27]: Exclua isto se você estiver

Commented [AES28]: Se por qualquer motivo o aceite do risco

Commented [AES29]: Você pode encontrar um modelo para

O [cargo] irá documentar os resultados da avaliação e do tratamento de riscos e todas a revisões subsequentes no Relatório de avaliação e tratamento de riscos.

[redacted]

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	*Responsável pelo armazenamento*	*Controles para proteção do registro*	*Tempo de retenção*
Tabela de avaliação de riscos (formato eletrônico – documento em Excel)	Computador de [cargo]	[cargo do proprietário da Tabela de avaliação de riscos]	Somente o [cargo] tem o direito de adicionar entradas e fazer alterações na Tabela de avaliação de riscos.	Os dados são armazenados permanente mente.
Tabela de tratamento de riscos (formato eletrônico – documento em Excel)	Computador de [cargo]	[cargo do proprietário da Tabela de tratamento de riscos]	Somente o [cargo] tem o direito de adicionar entradas e fazer alterações na Tabela de tratamento de riscos.	Os dados são armazenados permanente mente.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Commented [AES30]: Ex.: gerente de continuidade de [redacted]

Commented [AES31]: Ex.: gerente de continuidade de [redacted]

Commented [AES32]: Ex.: CEO, responsável pela unidade [redacted]

Commented [AES33]: Isso é apenas uma recomendação, [redacted]

Commented [AES34]: Insira uma data nesta coluna para [redacted]

Commented [AES35]: Ex.: gerente de continuidade de [redacted]

Commented [AES36]: Ex.: gerente de continuidade de [redacted]

Commented [AES37]: Exclua isto se você estiver [redacted]

Somente o [cargo] pode conceder aos demais funcionários [illegible]

Commented [AES38]: Ex.: gerente de continuidade de [illegible]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Commented [AES39]: Ex.: gerente de continuidade de [illegible]

Commented [AES40]: Isso é apenas uma recomendação, [illegible]

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- a quantidade de incidentes que ocorreram, mas não foram incluídos na avaliação de riscos
- a quantidade de riscos que não foram tratados adequadamente
- [illegible]

6. Anexos

- Anexo 1 – Tabela de avaliação de riscos
- [illegible]
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES41]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.