Gestão de Riscos de Segurança da Informação

Sumário

1 Objetivo 2

2 Atividades 2

2.1 CONTEXTO 2

2.2 IDENTIFICAÇÃO DE RISCOS 3

2.3 ANÁLISE E TRATAMENTO DE RISCOS 3

2.4 GERENCIAMENTO DE RISCOS 3

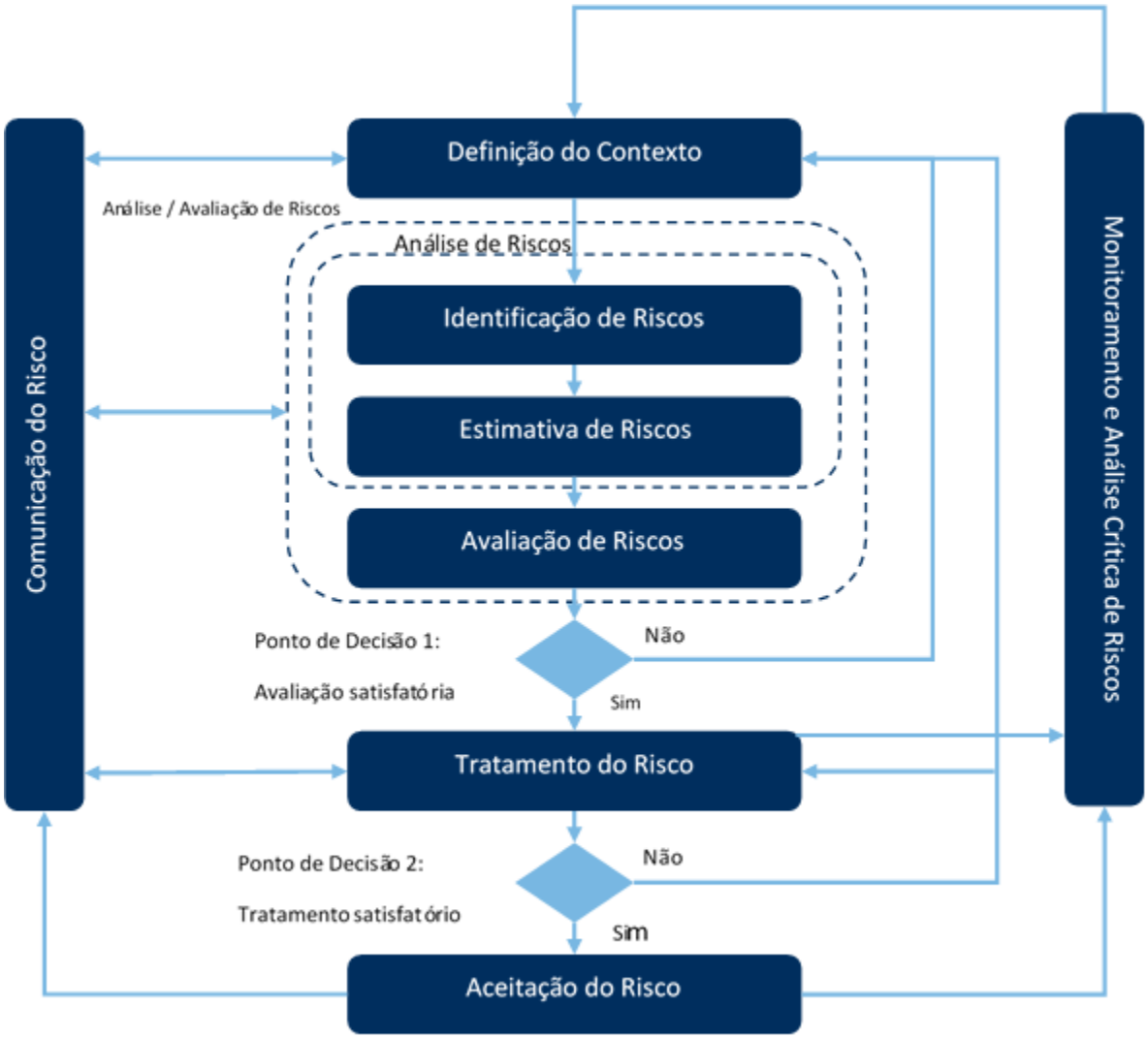
2.5 CICLO PDCA 4

3 Ferramenta 4

1 OBJETIVO

Estabelecer os princípios básicos, diretrizes e as melhores práticas no processo de gestão, análise e avaliação dos riscos relacionados à segurança da informação de modo a oferecer serviços sem paralização ou falhas.

2 ATIVIDADES



2.1 CONTEXTO

Ameaças podem ser intencionais ou acidentais e podem se relacionar tanto ao uso e aplicação de sistemas de TI como aos seus aspectos físicos e ambientais.

2.2 Identificação de riscos

Ameaças podem assumir diversas formas desde furto de mídia, documentos e equipamentos, forjamento de direitos, espionagem a distância, escuta não-autorizada, até fenômenos climáticos e sísmicos, incêndio, inundação e radiação eletromagnética.
Após a identificação dos riscos são realizadas as estimativa e avaliação dos mesmos.

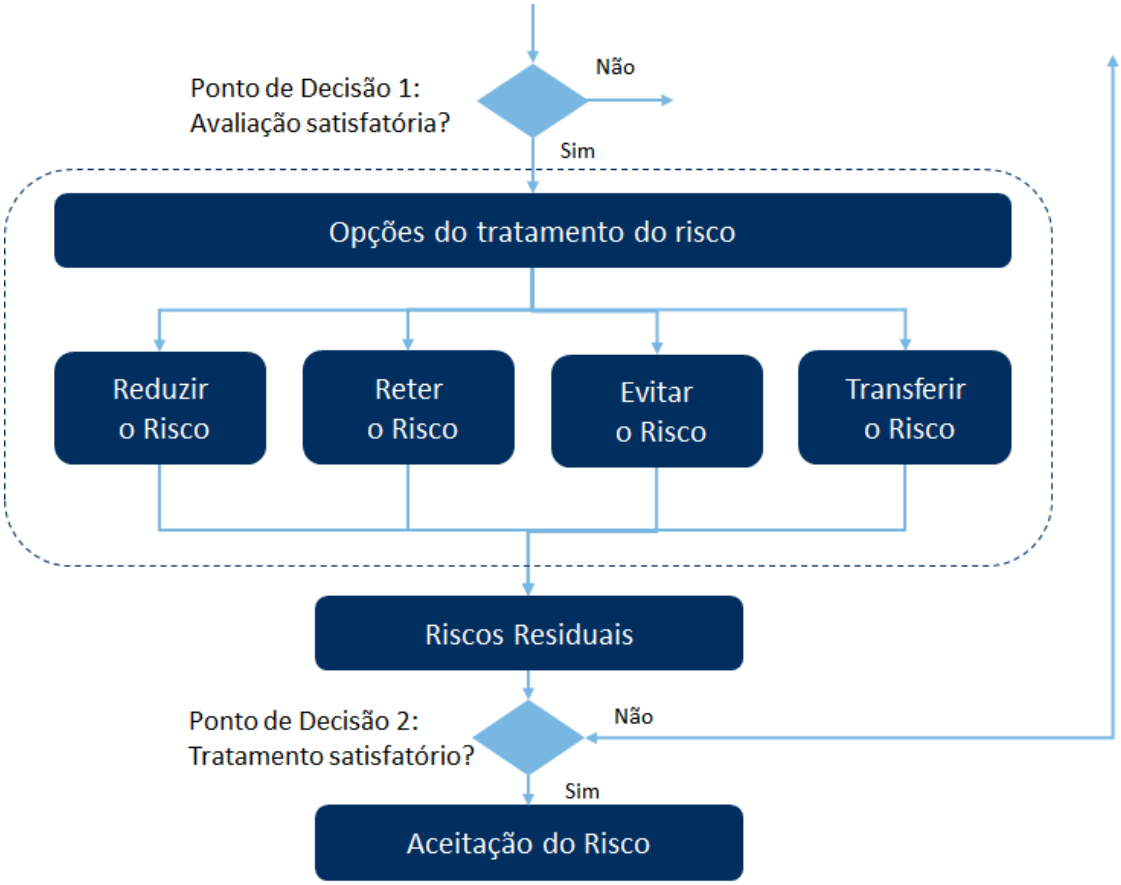
2.3 Análise e Tratamento de riscos

Na avaliação dos riscos quantificamos e descrevemos qualitativamente um risco de modo a priorizar os riscos de acordo com a sua severidade ou com outros critérios estabelecidos pela organização. Esta atividade consiste na consideração das fontes de riscos, nos eventos potenciais, suas consequências e probabilidade.
As atividades de análise, validação e tratamento dos riscos podem ser realizadas mais de uma vez.
O tratamento é iniciado quando a avaliação indicar e utiliza as ações identificadas e definidas no processo de avaliação.

2.4 Gerenciamento de Riscos

O gerenciamento de riscos está focado na criação de valor e proteção das informações é um processo dinâmico e segue as seguintes etapas:

- Definição do Plano
- Discussão dos riscos com feedback dos stakeholders
- Definição do escopo, contexto e critérios para abordagem
- Conclusão dos levantamentos do risco
- Tratamento dos riscos que afetam o atingimento das metas
- Reavaliar e melhorar o processo de gerenciamento de riscos



2.5 CICLO PDCA

O processo de gestão de riscos segue o ciclo PDCA:

- **P**lan: Definição do contexto, análise e avaliação dos riscos, definição do plano de tratamento;
- **D**o: Implementação do plano de tratamento do risco;
- **C**heck: Monitoramento contínuo e análise crítica de riscos;
- **A**ct: Manter, revisar e melhorar o processo de gestão de riscos de segurança da informação.

3 FERRAMENTA

A LOTE45 utiliza tabela FMEA como ferramenta para análise de riscos por atividade.