**Universidade de Brasília**
**Instituto de Ciências Exatas**
**Departamento de Ciência da Computação**

# Proposta de Metodologia de Gestão de Riscos para as Contratações de TI da Funasa

Leonardo Santana Nobre

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientadora
Prof.a Dr.a Ana Carla Bittencourt Reis

Brasília
2017

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Nobre, Leonardo Santana
NN754p Proposta de metodologia de gestão de riscos para as contratações de TI da Funasa / Leonardo Santana Nobre; orientador Ana Carla Bittencourt Reis. -- Brasília, 2017.
138 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2017.

1. Gestão de riscos. 2. Modelos de gestão de riscos. 3. Aquisições de TI. 4. Instrução Normativa n. 04. I. Bittencourt Reis, Ana Carla, orient. II. Título.

**Universidade de Brasília**
**Instituto de Ciências Exatas**
**Departamento de Ciência da Computação**

# Proposta de Metodologia de Gestão de Riscos para as Contratações de TI da Funasa

Leonardo Santana Nobre

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof.a Dr.a Ana Carla Bittencourt Reis (Orientadora)
EPR/UnB

Prof. Dr. Eduardo Amadeu Dutra Moresi
Universidade Católica de Brasília

Prof.a Dr.a Simone Borges Simão Monteiro
EPR/UnB

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 08 de agosto de 2017

# Dedicatória

Dedico este trabalho à Deus, por me permitir mais essa conquista, à minha família por estar ao meu lado em todos os momentos e à minha noiva pela paciência e incentivo.

# Agradecimentos

Agradeço à Deus em primeiro lugar, a todos aqueles que colaboraram de alguma maneira para a conclusão deste trabalho, à minha orientadora, aos professores, aos colegas do mestrado, aos coordenadores e membros da Coordenação Geral de Modernização e Tecnologia da Informação da Funasa, por me permitirem pesquisar meios para melhoria dos processos de trabalho. Quero agradecer também ao meu irmão pelas críticas, aos meus amigos, minha noiva, e à minha família pela compreensão durante toda essa jornada.

# Resumo

O processo de gestão de riscos nas contratações de Tecnologia da Informação (TI), fornece aos gestores um entendimento das ameaças que podem afetar o sucesso dos projetos de aquisição de TI, permitindo aos gestores reduzir problemas e alcançar seus objetivos estratégicos. Este trabalho visa propor a elaboração de uma metodologia para gestão de riscos dos processos de aquisições de TI da Fundação Nacional de Saúde (FUNASA). As contratações de TI da Funasa envolvem grandes volumes financeiros e apresentam riscos que influenciam negativamente as aquisições de TI do órgão. Problemas com riscos não gerenciados e sem evidências de controles, trouxeram, nos últimos anos, consequências indesejadas ao órgão, como a falta de equipamentos e serviços de TI, falta de reposição do material de consumo para os equipamentos, falta de suporte especializado para atender ao órgão e a impossibilidade de atender as demais áreas da instituição em seus projetos. A metodologia proposta por este trabalho apresenta um estudo de caso, com uma pesquisa aplicada a partir da realidade diagnosticada na organização, baseado na coleta de dados em documentos, leis, normas brasileiras, *frameworks*, normas internacionais como a ABNT NBR ISO 31000 e ABNT NBR ISO 31010 e modelos de gestão de riscos difundidos pela literatura, com o objetivo de fornecer insumos para a elaboração de um material de referência para os envolvidos no processo de contratação de TI da FUNASA. O trabalho propõe uma abordagem sistêmica, apresentando conceitos, processos, atividades, tarefas e artefatos para integrar a gestão de riscos das contratações de TI, contribuindo para a normatização de procedimentos e a melhoria nos resultados das contratações de TI dentro da realidade da FUNASA. Os resultados apresentados demonstram que a metodologia proposta apresenta viabilidade para sua utilização nos órgãos públicos federais como meio de auxiliar a internalização de procedimentos previstos na legislação e o aprofundamento do tema de gestão de riscos nas contratações de TI na Administração Pública Federal (APF).

**Palavras-chave:** Gestão de riscos, modelos de gestão de riscos, aquisições de TI, Instrução Normativa nº 04 (SLTI/MP).

# Abstract

The risk management process in IT hiring provides managers with an understanding of the threats that can affect the success of IT acquisition projects, allowing managers to reduce problems and achieve their strategic objectives. This paper aims at proposing the elaboration of a methodology for risk management of the IT acquisition processes of the National Health Foundation (FUNASA). Funasa's IT hiring involves large financial volumes and presents risks that negatively influence the company's IT acquisitions. Problems with unmanaged risks and no evidence of controls have led, in recent years, to unintended consequences for the agency, such as a lack of IT equipment and services, lack of replacement of consumables for equipment, lack of specialized support to And the impossibility of attending to the other areas of the institution in its projects. The methodology proposed by this work presents a case study, with a research applied based on the reality diagnosed in the organization, based on the collection of data in documents, laws, Brazilian standards, frameworks, international standards such as ISO 31000 and ABNT NBR ISO 31010 and management models Of risks disseminated in the literature, aiming to provide inputs for the elaboration of a reference material for those involved in FUNASA's IT contracting process. The work proposes a systemic approach, presenting concepts, processes, activities, tasks and artifacts to integrate the risk management of IT contracting, contributing to the standardization of procedures and improvement in the results of IT contracting within FUNASA's reality. The results show that the proposed methodology presents feasibility for its use in federal public agencies as a means of assisting the internalization of procedures provided for in the legislation and the deepening of the topic of risk management in IT contracting in the Federal Public Administration (APF).

**Keywords:** Risk management, risk management models, acquisitions of TI, Normative Instruction nº 04 (SLTI/MP).

# Sumário

# Lista de Figuras

# Lista de Quadros

# Lista de Abreviaturas e Siglas

**APF** Administração Pública Federal.

**CF88** Constituição Federal de 1988.

**CGIBR** Comitê Gestor da Internet no Brasil.

**CGMTI** Coordenação Geral de Modernização e Tecnologia da Informação.

**CGU** Controladoria Geral da União.

**COBIT** Control Objectives For Information and Relatet Technology.

**COINF** Coordenação de Sistemas de Informação.

**COINT** Coordenação de Inovação e Infraestrutura Tecnológica.

**DOD** Documento de Oficialização da Demanda.

**FUNASA** Fundação Nacional de Saúde.

**IN-SLTI/MP 04** Instrução Normativa nº 4.

**INC-CGU/MP 01/2016** Instrução Normativa Conjunta nº 1.

**IRM** Institute Risk Management.

**MCTI** Modelo de Contratação de TI.

**MP** Ministério do Planejamento.

**OGS** Órgãos Governantes Superiores.

**PDTI** Plano Diretor de Tecnologia da Informação.

**PETI** Plano Estratégico de TI.

**PMBOK** Project Management Body of Knowledge.

**PMI** Project Management Institute.

**PPA** Plano Plurianual da FUNASA.

**SIC** Segurança da Informação e Comunicações.

**SISP** Sistema de Administração de Recursos da Tecnologia da Informação.

**SLTI** Secretaria de Logística e Tecnologia da Informação.

**STI** Secretaria de Tecnologia da Informação.

**TCU** Tribunal de Contas da União.

**TI** Tecnologia da Informação.

# Capítulo 1

# Introdução

## 1.1 Contextualização

A utilização de recursos de Tecnologia da Informação (TI), nos dias atuais, é considerada imprescindível para que o setor público viabilize a implementação de processos inovadores e aumente a capacidade do governo de melhorar a prestação dos serviços aos cidadãos. Cada vez mais pessoas e empresas dão preferência ao uso de serviços *on-line* e à conveniência dos ambientes virtuais para a solicitação de seus serviços governamentais. Tal comportamento é explicado, em parte, pela agilidade que tais ambientes oferecem aos usuários na resolução das requisições, esse cenário, faz com que surjam, cada vez mais, demandas de investimentos em tecnologia nas instituições públicas e, consequentemente, cresça o esforço dos órgãos de controle no acompanhamento da correta aplicação dos recursos públicos [20].

No âmbito da Administração Pública Federal (APF), as contratações de soluções de TI demandam grandes volumes financeiros, aproximadamente 17 bilhões de reais em 2014 e 20 bilhões de reais em 2015, e tratam de itens estratégicos, de importância e relevância para a missão dos órgãos governamentais, que geram valor ao negócio com projetos ligados ao alcance dos objetivos institucionais [21, 29].

Neste contexto, tendo em vista o crescimento da área e da importância que tem assumido na APF, além do consequente aumento do número de aquisições de soluções para o atendimento da demanda, muitos órgãos da APF têm apresentado recorrentes contratações malsucedidas, indicadas principalmente, pelas ações de controle do Tribunal de Contas da União (TCU), como demonstrado nos acórdãos 1.603 de 2008, 2.471 de 2008, 2467 de 2013, 3.137 de 2014 e 916 de 2015, os quais relatam as principais limitações que as instituições públicas têm encontrado na condução de suas contratações de TI [28, 29].

Os problemas identificados pelo TCU nas contratações de TI, vão de falhas na justificativa do objeto, na definição do volume de serviços a serem contratados, no detalhamento

das sanções administrativas, nos artefatos produzidos, até a ausência de rastreamento dos serviços prestados, pagamento por serviços não prestados, falta de avaliação dos serviços e desconformidade na aplicação dos critérios de medição, além de inúmeras fragilidades que fazem com que o TCU recomende, reiteradamente, aos órgãos superiores, a criação de abordagens para melhoria dos resultados pretendidos com as contratações de TI no âmbito da APF [23].

Desde 2008 a Secretaria de Logística e Tecnologia da Informação (SLTI)[1] do Ministério do Planejamento (MP), atenta às recomendações do TCU, tem buscado a normatização e padronização das contratações de TI dos órgãos públicos federais, com a publicação de normas, tais como a Instrução Normativa nº 4 (IN-SLTI/MP 04), e de manuais, como o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação, que descrevem uma série orientações para as contratações de TI na APF. Estes documentos auxiliam os envolvidos no processo de contratação de TI, no entendimento dos passos, atores e artefatos a serem considerados nas contratações de TI e ampliam as orientações sobre o tema [34].

Tal normatização relacionada às contratações de TI na APF, tem reservado grande importância para a gestão de riscos, como instrumento de controle dos gastos públicos e contribuição para que as instituições obtenham boas práticas na gestão dos recursos de TI. A gestão de riscos nas contratações de TI é parte necessária para a agregação de valor aos órgãos públicos, e deve ser, cada vez mais, explorada e discutida para a melhoria contínua dos serviços prestados à sociedade.

## 1.2 Definição do Problema

A Fundação Nacional de Saúde (FUNASA), fundação pública vinculada ao Ministério da Saúde, vem enfrentando dificuldades em suas contratações de TI, seja pelo reduzido número de pessoal envolvido, seja pela necessidade de melhoria do gerenciamento dos projetos de contratação de serviços e produtos de tecnologia. A FUNASA possui capilaridade em todas as unidades federativas, contudo, praticamente toda aquisição em TI é centralizada na presidência da FUNASA, localizada em Brasília, de maneira que, as compras de TI que não são concluídas, impactam diretamente as ações finalísticas do órgão e da população em todo país.

Pelo menos nos últimos 3 anos, algumas contratações de TI do órgão foram frustradas, resultando em atrasos na prestação de serviços, falta de produtos e paralisação de equipamentos. Esse fato gerou consequências indesejadas na instituição como: falta de

[1]Com nomenclatura alterada após o decreto 8.578 de 26 de novembro de 2015 passa a se chamar Secretaria de Tecnologia da Informação (STI) do Ministério do Planejamento, contudo, as normas editadas antes da mudança citada manterão a sigla SLTI.

atualização do parque computacional, falta de reposição do material de consumo para os equipamentos, falta de suporte especializado para atender ao órgão, impossibilidade de atender as demais áreas da instituição em seus projetos, falta de suporte e garantia para os equipamentos de TI e problemas no gerenciamento nas contratações de TI.

Os riscos das contratações de TI na FUNASA, atualmente, não são efetivamente gerenciados. Não há um estudo para a identificação, construção de uma base de conhecimentos ou criação de controles ou indicadores sobre as possíveis ameaças e vulnerabilidades das contratações. Em 2015, por exemplo, as contratações dos serviços de *outsourcing* de impressão e serviços especializados de suporte ao usuário não foram finalizadas, o que provocou a interrupção da prestação desses serviços por alguns meses do ano de 2015. O problema no processo de contratação foi decorrente de procedimentos recursais licitatórios (questionamentos, impugnações e recursos das empresas concorrentes), que são meios nos quais os licitantes possuem para impugnar administrativamente as decisões das licitações, mas apontam riscos que, se não cuidadosamente tratados e controlados, comprometem o objetivo de uma aquisição bem-sucedida. Uma vez que, nos dias atuais, a TI é primordial, e muitas vezes condicionante do sucesso dos processos organizacionais, a ausência dos serviços de impressão e de suporte ao usuário provocaram impactos significativos no desempenho das atividades dos usuários dos serviços de TI, comprometendo, as atividades fim da FUNASA, dedicadas ao cumprimento da sua missão de garantir a saúde do cidadão e projetos que beneficiam a população.

Apesar do grande avanço vindo da adoção da IN-SLTI/MP 04 em suas normas internas de contratação de TI pela FUNASA, a norma ainda deixa lacunas para serem preenchidas pelos órgãos. Um dos problemas enfrentados por essas lacunas na FUNASA é a falta de orientação prática no gerenciamento dos riscos nas contratações de soluções de TI. A norma não detalha as atividades a serem tomadas para uma gestão efetiva dos riscos e, dessa forma, para atender aos requisitos propostos pela norma e tornar o controle dos riscos eficaz, as organizações devem utilizar um conjunto de ferramentas e técnicas de gestão de riscos que auxiliem nesse objetivo.

Neste sentido, o processo de gestão de riscos proposto pela norma apresenta alguns aspectos negativos. Dentre eles destacam-se [75]:

1. O modelo não é claro, podendo ter várias interpretações. Cada integrante da equipe pode interpretar de um jeito e analisar os riscos da sua maneira, gerando contratações do mesmo produto, com levantamento de riscos completamente distintos, ocasionando contratos bem elaborados ou pouco especificados;

2. Não existem documentos explicativos que os gestores possam consultar, para entender qual é o conceito de riscos, impacto e probabilidade;

3. Não há garantia de que os principais pontos da contratação serão considerados na análise riscos, não existe um padrão ou instrumento facilitador para tal;

4. Cada organização deve utilizar os seus padrões específicos, normas ou procedimentos e técnicas que tratem em detalhe os elementos da gestão de riscos das contratações.

Além disso, outros pontos poderiam ser citados, como o fato da análise dos riscos não ser revisada e assim gerar análises obsoletas, não gerar bases de conhecimento para novas contratações, o processo não ser automatizado podendo gerar distorções nas contratações, não considerar riscos políticos, entre outros. A FUNASA não possui uma metodologia que estabeleça e padronize as atividades de gestão de riscos nas contratações de TI, com adoção de ferramentas, boas práticas, e técnicas amplamente utilizadas que uniformizem todo processo [35, 75].

Este trabalho visa apresentar uma metodologia para a gestão de riscos das contratações de TI, com a aplicação de conhecimentos da literatura acadêmica, técnicas, controles, ferramentas ou normas que possibilitem a melhoria do processo de gestão dos riscos das contratações de TI da FUNASA.

## 1.3 Justificativa do Tema

A notória expansão da TI nos últimos anos, tem levado a um significante crescimento no volume das suas aquisições no âmbito da administração pública. Este fato fez surgir um grande e complexo número de normativos, que visam padronizar os requisitos nos processos de contratação. Os serviços suportados pela área de TI servem para manter em funcionamento as operações e funções dos órgãos públicos, apoiando seus processos finalísticos. A paralisação ou descontinuidade de algum produto ou serviço de TI expõem a administração ao risco de não atingimento de seus objetivos estratégicos institucionais [19].

As orientações recentes do TCU têm recomendado aos Órgãos Governantes Superiores (OGS) que emitam orientações acerca das práticas de governança de TI a serem adotadas pelas instituições a eles vinculadas, contudo, a despeito dos esforços realizados muitas instituições demonstram dificuldades em identificar quais caminhos devem trilhar na implementação de processos, controles e aplicação das normas já existentes [28].

No último levantamento sobre governo eletrônico, o Comitê Gestor da Internet no Brasil (CGIBR), identificou em um levantamento com 1.386 órgãos públicos federais e estaduais em 2015, que mais de 40% dos órgãos públicos não possuem processos de gestão de riscos relacionados à TI. Nos órgãos do poder Executivo esse índice chega à 65% [20].

Além disso, em recente auditoria, o acórdão nº 916 de 2015, o TCU encontrou desconformidades na gestão de riscos das contratações de TI dos órgãos da APF, com a conclusão que os riscos elencados no planejamento das contratações são uma maneira estritamente formal de inclusão do documento "Análise de Riscos", descrito no art. 13 da IN-SLTI/MP 04, sem produção eficaz de controles e resultados para o órgão [29].

A criação de normas, auditorias e orientações bem específicas para o processo de contratação de soluções de TI na APF, demonstra que tal processo possui peculiaridades e características que o distingue dos demais processos de aquisições governamentais, caso contrário, as demais legislações vigentes dedicadas à regulação das contratações em geral, seriam suficientes. A falta de um instrumento que uniformize o entendimento da gestão de riscos das contratações impacta diretamente a capacitação, já precária, dos servidores designados como gestores e fiscais responsáveis pela aquisição de bens e serviços de TI [14].

Entretanto, apesar dos claros avanços institucionais relacionados ao desenvolvimento da IN-SLTI/MP 04, da publicação do Guia de Boas Práticas em Contratação de Soluções de TI, da Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações e demais esforços na capacitação de servidores públicos com foco na adoção de melhores práticas nesse contexto, observa-se uma lacuna com relação ao acompanhamento e fiscalização da real adoção dos processos propostos [38].

Para que a administração consiga governar a TI de forma a atender às necessidades institucionais, é necessário que ela estabeleça um conjunto de princípios, diretrizes, ferramentas, técnicas e *frameworks* que orientem o comportamento desejado e estabeleçam um padrão de atuação na contratação, gestão e no uso da TI institucionalmente [28]. A utilização das normas e leis instituídas, em conjunto com métodos e estudos científicos em gestão de riscos podem ajudar a FUNASA a planejar, acompanhar e monitorar todo processo de contratação e os riscos inerentes a ele de maneira eficaz, eficiente e efetiva, reduzindo a ocorrência de problemas relacionados aos projetos de TI.

O presente trabalho, utilizando como estudo de caso a FUNASA, que possui complexa estrutura tecnológica a ser mantida com as aquisições de TI, apresenta uma proposta de metodologia que tem por objetivo proporcionar a melhor utilização da TI para o órgão, gerenciando os riscos, estando em conformidade legal e agregando valor aos objetivos estratégicos [24].

A elaboração e posterior utilização da metodologia pretende apoiar o gerenciamento das incertezas, ameaças e vulnerabilidades, oferecendo maior controle dos riscos identificados com o suporte de um material de referência, direcionada aos profissionais que atuam no planejamento da contratação, gerando melhor chance de entrega dos serviços no prazo, no custo e na qualidade esperada, redução de problemas, crises, aumento de chances de

sucesso de programas e projetos governamentais e maior transparência [34].

A metodologia visa padronizar e sistematizar a gestão de riscos na FUNASA, o que permitirá a organização ter dados claros para direcionar ações na otimização de atividades pouco maduras e focar na conscientização dos funcionários quanto à importância da área da gestão de riscos que atualmente não é vista com a devida importância para as contratações de TI.

Tais ações, proporcionadas pelos resultados deste trabalho, serão fundamentais em uma gestão de risco mais eficiente no processo de contratação de TI da FUNASA. Isso significa um processo mais robusto, menos vulnerável aos impactos dos riscos inerentes às contratações, resultando em uma maior efetividade no gasto dos recursos públicos.

### 1.3.1 Objetivo Geral

Propor a elaboração de uma metodologia de gestão de riscos para o processo de contratação de TI da FUNASA.

### 1.3.2 Objetivos Específicos

- Pesquisar modelos de gestão de riscos amplamente utilizados;
- Pesquisar métodos, técnicas e ferramentas sistêmicas para compor a metodologia de gestão de riscos das contratações de TI da FUNASA;
- Definir os processos que irão compor a metodologia de gestão de riscos das contratações de TI da FUNASA;
- Elaborar as atividades, tarefas, artefatos e definir os papéis dos atores envolvidos para a construção da metodologia de gestão de riscos das contratações de TI da FUNASA.

### 1.3.3 Contribuição esperada

A contribuição esperada é que o trabalho de pesquisa seja utilizado como material de referência para os envolvidos no processo de contratação de TI da FUNASA, reduzindo a probabilidade de impactos negativos sobre os projetos de contratação de TI do órgão. A proposta de metodologia de gestão de riscos para as contratações de TI da FUNASA deve responder algumas questões de pesquisa como: quais os modelos de gestão de riscos, encontrados na literatura, podem ser utilizados como base para a elaboração de uma proposta de metodologia de gestão de riscos nas contratações de TI na FUNASA? quais

técnicas de gestão de riscos, encontrados na literatura, podem ser utilizadas para a proposta de metodologia? quais atividades e tarefas devem ser executadas na gestão de riscos das contratações de TI da FUNASA? quais as entradas, saídas e requisitos para as atividades da gestão de riscos nas contratações de TI da FUNASA? quais os papéis e responsabilidades do processo de gestão de riscos das contratações de TI da FUNASA?

Tal proposta de metodologia tem por objetivo tornar a gestão de riscos das contratações de TI do órgão uma realidade, estando assim em conformidade legal e proporcionando melhoria nos processos internos relacionados às contratações de TI do órgão. A pesquisa busca o amadurecimento do órgão com relação às contratações de TI, contribuindo para o nivelamento de procedimentos e de boas práticas, oferecendo maior controle dos riscos identificados e melhor chance de conclusão dos projetos de contratação de TI na FUNASA.

### 1.3.4 Estruturação dos Capítulos

O trabalho está estruturado em seis capítulos, com objetivo de demonstrar a construção da metodologia de gestão de riscos das contratações de TI da FUNASA de maneira evolutiva. O Capítulo 1 trata da Introdução, trazendo a contextualização, definição do problema, a justificativa do tema com apresentação dos objetivos da presente pesquisa. No Capítulo 2 é apresentado a base conceitual e revisão da literatura, onde são descritos as pesquisas relacionadas ao tema da gestão de riscos e contratações de TI que contribuirão para formação no entendimento sobre o assunto e na formação da metodologia proposta. O segundo capítulo descreve ainda conceitos, definições e características relevantes de modelos e técnicas de gestão de riscos amplamente utilizados e com uma possível aderência ao processo de contratações de TI. Também são abordadas as atuais legislações governamentais relacionadas à gestão de riscos na APF, dando destaque especial à IN-SLTI/MP 04 por ser considerada a principal norma sobre assunto de contratações de TI na APF. O Capítulo 3 apresenta a metodologia científica com os métodos e as técnicas de pesquisa utilizadas. O Capítulo 4 descreve o estudo de caso com o contexto no qual está inserido a pesquisa, com uma análise da situação atual do objeto de estudo. O Capítulo 5 propõe a elaboração do da metodologia de gestão de riscos para as contratações de TI na Funasa a partir do diagnóstico e da revisão de literatura. O Capítulo 6 apresenta conclusão do trabalho. Ao final, as referências bibliográficas e os apêndices com os artefatos elaborados durante a pesquisa.

# Capítulo 2

# Base Conceitual e Revisão de Literatura

Este capítulo contém informações sobre as principais disciplinas, métodos e técnicas envolvidas no tema da pesquisa. Para isso, é apresentado informações referentes à gestão de riscos, modelos e técnicas de gestão de riscos e normas referentes às aquisições de TI no setor público. Considerando os objetivos principal e específicos deste trabalho, a literatura de gestão de risco é analisada sob o aspecto das contratações públicas, mais especificamente, as contratações de bens e serviços de TI.

## 2.1 Riscos

O conceito de risco que se conhece atualmente provém da teoria das probabilidades na qual considera a previsibilidade de determinadas situações ou eventos por meio do conhecimento de acontecimentos futuros [30]. Tal previsibilidade leva em conta as incertezas relacionadas, e o risco é a exposição às consequências da incerteza, é a chance de algo acontecer que tenha um impacto sobre uma finalidade. Isto inclui a possibilidade de perda ou ganho, ou a variação de um resultado desejado ou planejado como consequência da incerteza associada a determinada ação. O risco, portanto, tem dois elementos: a probabilidade de algo acontecer e as consequências ou impactos relacionados [18].

Nas organizações, os riscos são os fatores e as influências que tornam incerto o cumprimento de seus objetivos institucionais [54]. O *Project Management Institute (PMI)* afirma que *"risco é um evento ou condição incerta, que se ocorrer, provocará um efeito positivo ou negativo nos objetivos do projeto"* [67]. Os riscos positivos são considerados oportunidades para as organizações (melhoria nos processos, aumento de produtividade, ganhos financeiros), enquanto os riscos negativos geram perdas (financeiras, danos à imagem da instituição, paralisação de serviços, entre outros) [59].

Esses riscos positivos e negativos ocorrem da combinação da probabilidade de um evento ocorrer e suas consequências. Segundo o PMI, os riscos positivos e negativos são conhecidos através de um processo de identificação e análise que possibilite o planejamento de respostas. Com a identificação, os riscos podem ser priorizados e classificados, já a etapa de análise acompanha os riscos a partir do grau de impacto, da probabilidade de ocorrência, das ameaças que geram para as organizações, dispondo assim, das incertezas dos eventos em um ambiente que possa ser controlado e gerenciado [67].

Dessa maneira, a gestão de riscos é, cada vez mais, reconhecida como a disciplina preocupada com os efeitos das incertezas sobre os objetivos da organização, buscando minimizar as consequências negativas, focando na prevenção e mitigação de prejuízo e maximizando a melhoria contínua dos processos organizacionais [82].

## 2.2 Gestão de Riscos

Um dos primeiros estudos científicos no qual o termo gestão de riscos foi mencionado, surgiu em 1985 por Otway, nele o autor percebendo as transformações da sociedade e suas implicações diretas e indiretas nos custos financeiros gastos pelo Estado e pelas indústrias, concluiu que a gestão de riscos e das incertezas era indispensável para o alcance dos objetivos nas organizações públicas e privadas [66].

Essa percepção ajudou as organizações a criarem mecanismos de controle sobre os eventos que impactassem negativamente seus negócios, emergindo assim, a gestão de riscos. O objetivo da gestão de riscos é, através da utilização de políticas, planos, responsabilidades, processos, métodos e ferramentas, criar um quadro de referência que permita às organizações lidarem com o risco e a incerteza sobre seus objetivos [33].

As ações da gestão de riscos estão ligadas à diferentes campos de pesquisa, mas a literatura acadêmica geralmente associa o gerenciamento de riscos ao gerenciamento de projetos [69]. Tinnirello (2001) afirma que existem duas abordagens para alcançar o sucesso do projeto: o gerenciamento de projetos e o gerenciamento de riscos [79]. O gerenciamento de riscos é fator crítico de sucesso em projetos, e as organizações tem o desafio de saber lidar com as situações de risco devido a suas características peculiares ao longo do projeto [22].

A gestão de riscos nos projetos deve ser entendida como item estratégico de todas as áreas organizacionais, pois contribui para o retorno de bons resultados e melhoria constante no desempenho do negócio [15]. Assim, também a área de TI deve estar atenta em gerenciar os riscos associados a seus projetos internos [17]. A incapacidade de lidar com o risco é considerada também uma das principais causas para que projetos tenham seu orçamento excedido [13]. Nos investimentos em TI, esta situação é exacerbada porque os

projetos são de grandes aportes financeiros, longos processos de execução, muitos recursos, interessados e ambientes econômico e político com alto nível de complexidade [49]. Portanto, há uma forte necessidade de avaliar e controlar o risco nas fases de um projeto de TI para reduzir prejuízos futuros.

A norma ABNT NBR ISO 31000 (2009), apresenta que a gestão dos riscos, quando implementada, possibilita a uma organização os seguintes benefícios [53]:

- Aumentar a probabilidade de atingir os objetivos;
- Encorajar uma gestão proativa;
- Estar atento para a necessidade de identificar e tratar os riscos através de toda a organização;
- Melhorar a identificação de oportunidades e ameaças;
- Atender às normas internacionais e requisitos legais e regulatórios pertinentes;
- Melhorar o reporte das informações financeiras;
- Melhorar a governança;
- Melhorar a confiança das partes interessadas;
- Estabelecer uma base confiável para a tomada de decisão e o planejamento;
- Melhorar os controles;
- Alocar e utilizar eficazmente os recursos para o tratamento de riscos;
- Melhorar a eficácia e a eficiência operacional;
- Melhorar o desempenho em saúde e segurança, bem como a proteção do meio ambiente;
- Melhorar a prevenção de perdas e a gestão de incidentes;
- Minimizar perdas;
- Melhorar a aprendizagem organizacional; e
- Aumentar a resiliência da organização.

Dessa forma, gerenciar os riscos exige a aplicação de metodologias adequadas, que integrem conhecimentos de vários campos da gestão e uma grande variedade de técnicas e ferramentas que deem suporte a problemas específicos [3]. Nesse sentido, também os especialistas do governo começaram a desenvolver e aplicar métodos científicos para estimar os riscos de modo quantitativo e probabilístico em seus produtos e processos [72]. As

organizações públicas devem aderir a uma estrutura de gestão de riscos, para minimizar o impacto dos eventos negativos à suas ações, aperfeiçoando sua prestação de serviços à sociedade.

## 2.3 Gestão de Riscos na Administração Pública Federal

No Brasil, são poucos os órgãos e entidades públicas que possuem políticas ou práticas de gestão de riscos formalmente estabelecidas. Essa lacuna, torna a gestão de risco no setor público um desafio a ser conquistado. Muitos passos devem ser percorridos, além da exigência legal imposta, para demonstrar que o gerenciamento dos riscos nas instituições públicas pode contribuir para determinar os fatores que ameaçam seus objetivos e para encontrar o melhor valor para os cidadãos, prestando o serviço público da melhor maneira possível [31].

As matérias referentes à gestão de riscos, governança e controles internos são temas relativamente recentes na formação da APF brasileira, considerando seus quase 30 anos de democracia, mas crescem na demanda dos órgãos, para dar suporte à organização e monitorar a realização de suas ações [1].

Diversos esforços estão sendo realizados no sentido de propagar uma cultura de riscos na APF, entre seus gestores e agentes públicos. Atualmente, existem diversos documentos publicados que fazem referências a gestão de riscos na administração pública e ajudam a criar uma melhor compreensão do tema. Dentre eles, podemos destacar a Constituição Federal de 1988 (CF88), que no seu artigo 74, trata do controle interno e a ênfase na verificação da eficácia e eficiência quando da avaliação de resultados da gestão pública e documentos como o Guia de Orientação para o Gerenciamento de Riscos, a Metodologia de Gestão de Riscos do SISP, e a Instrução Normativa Conjunta nº 1 (INC-CGU/MP 01/2016) que serão abordados nas seções seguintes [43].

### 2.3.1 Guia de Orientação para o Gerenciamento de Riscos

A Secretaria de Gestão Pública do Ministério do Planejamento lançou em 2013, um guia de orientação para o gerenciamento de riscos, sendo um dos primeiros documentos que se referem diretamente à gestão de riscos na APF. O documento elenca os fundamentos e as etapas que devem ser levadas em consideração para o gerenciamento de riscos, assim como provém um direcionamento para aqueles envolvidos na avaliação de riscos, auditoria interna e liderança das organizações públicas [34].

A estrutura do guia, com seus conceitos e princípios, foi baseada no modelo do *"The Orange Book"* produzido e publicado pelo ministério do tesouro ou finanças do Governo Britânico. O guia destaca que o gerenciamento de riscos é fundamental para o sucesso no cumprimento da missão da organização pública em entregar serviços de qualidade para o cidadão [34]. Dentre as vantagens que o guia apresenta, na adoção de um mecanismo de gerenciamento de riscos para as organizações públicas estão [34]:

- Melhoria na entrega de serviços ao cidadão;
- Melhor utilização de recursos; e
- Melhor planejamento e melhor gerenciamento de programas e projetos.

O guia é um importante documento para a introdução dos conceitos e terminologias empregadas na gestão de riscos nas instituições governamentais, auxiliando as lideranças a adotá-lo como apoio para implementar, de uma forma simples e eficaz, o gerenciamento de riscos na sua organização.

### 2.3.2 Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações - SISP

A Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração de Recursos da Tecnologia da Informação (SISP), do Ministério do Planejamento, foi lançada em 2016 com o objetivo de padronizar e sistematizar a gestão de riscos de Segurança da Informação e Comunicações (SIC) na APF. O guia auxilia os órgãos federais para elaboração de suas políticas de segurança da informação e na racionalização dos investimentos em TI [36].

A metodologia está em conformidade com outras leis, normas e documentos relacionados à gestão de riscos como a Norma Complementar nº 04 do Gabinete de Segurança Institucional da Presidência da República, Instrução Normativa Conjunta MP/CGU nº 1 e a NBR ISO 27005 [36].

A proposta apresenta um conjunto de 7 processos agrupados em 65 tarefas e 16 atividades voltadas para a gestão de riscos em ativos de segurança da informação, mas que podem ser adaptados para outros processos das instituições. Para elaboração da gestão de riscos, a metodologia prevê o envolvimento das autoridades competentes (representantes da alta direção, que aprovam pontos importantes da gestão de riscos), dos responsáveis pela gestão de riscos (a equipe que executará as atividades de gestão de riscos), dos responsáveis por avaliar as informações (integrantes que acompanham e realizam as melhorias necessárias no processo) e dos responsáveis pelas áreas da organização (nas quais a metodologia de riscos será implementada) [36].

Todos esses pontos apontam para uma metodologia bem estruturada que auxilia as instituições públicas do Governo Federal a implementarem políticas de gestão de riscos e segurança da informação, estabelecendo padrões e um conjunto de princípios e processos que auxiliem os gestores públicos a proteger os elementos de valor da organização.

### 2.3.3 Instrução Normativa Conjunta MP/CGU nº 1

A Controladoria Geral da União (CGU) e o Ministério do Planejamento (MP), buscando convergir as normas governamentais e as melhores práticas de gestão de riscos corporativas, editaram em 2016, a Instrução Normativa Conjunta nº 1 (INC-CGU/MP 01/2016), recomendando aos órgãos e entidades do poder executivo federal, a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança. Com a norma, os órgãos passam a serem responsáveis por uma série de controles, estratégias, estruturas de gerenciamento de riscos e monitoramento e o aperfeiçoamento dos controles internos da gestão. Dentre outras recomendações da norma, pode-se verificar que [37]:

1. Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado;
2. O agente responsável pelo risco deve ser um gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco;
3. As tipologias de risco abrangem: riscos operacionais, de imagem/reputação do órgão, legais e financeiros/orçamentários; e
4. A norma também prevê a instituição de comitês de governança, riscos e controles em todos os órgãos federais. Cada comitê será formado pelo dirigente máximo do órgão ou entidade, pelos dirigentes das unidades a ele diretamente subordinadas e será apoiado pelo respectivo assessor especial de Controle Interno.

Com a publicação da norma, os órgãos terão sob sua responsabilidade a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência, efetividade das informações, promovendo o desenvolvimento contínuo dos agentes públicos. Além disso, a norma busca garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas a condução das políticas e à prestação de serviços de interesse público, bem como supervisionar o mapeamento e avaliação dos riscos-chaves que podem comprometer a prestação de serviços de interesse público, entre outras atribuições [37].

A INC-CGU/MP 01/2016 traz uma grande contribuição para as organizações públicas quanto a inserir uma cultura de gestão de riscos em seus processos e projetos. Os esforços

apresentados pela referida norma, devem diminuir as lacunas encontradas por diversas auditorias dos órgãos de controle (acórdãos do TCU, 1.603/2008, 2.471/2008, 2467/2013, 3.137/2014, 916/2015 entre outros) que demonstram que os controles devem ser aprimorados para a efetiva aplicação nos órgãos da gestão de riscos em seus processos, como das contratações de TI.

### 2.3.4 Gestão de Riscos nas Contratações de TI da APF

As contratações de TI estão expostas à riscos que podem impactar diretamente as ações e objetivos finalísticos das organizações [83]. O grande dispêndio de valores em investimento de tecnologia faz com que os órgãos da APF corram o risco de gastar enormes quantias sem benefícios compatíveis em contrapartida, como o aprimoramento dos seus processos de trabalho [24].

O acórdão nº 2.622 de 2015 do TCU afirma que para buscar o melhor resultado para a organização, os órgãos devem estabelecer processos e modelos bem estruturados para a gestão de riscos nas aquisições de bens e serviços de TI [26]. O processo de contratação de TI deve ter especial destaque, pois [55]:

1. Trata-se de uma opção estratégica da área de TI;
2. Afeta diretamente a qualidade dos serviços de TI oferecidos aos clientes;
3. A área de TI continua a ser responsável pelos resultados dos serviços contratados; e
4. Afeta os custos da área de TI e, portanto, o valor agregado à organização.

A APF não possuía até 2008 uma lei ou norma unificada para regulamentar o processo de contratação de serviços ou recursos de TI no que diz respeito à compra ou contratação de serviços de informática ou comunicações, mas em 2008, com a edição da Instrução Normativa nº 4 (IN-SLTI/MP 04/2008) o processo de contratação de TI passou a ser disciplinado e a gestão de riscos começou a ser tratada como parte integrante do processo de contratação de TI [6].

O processo de trabalho para contratação de serviços e produtos de TI estabelecido na IN-SLTI/MP 04/2008 é dividido em três fases: planejamento da contratação, seleção do fornecedor e gestão do contrato [21]. A etapa referente ao gerenciamento de riscos do processo de contratação de TI está inserida dentro da fase de planejamento da contratação e é chamada de "Análise de Riscos" descrita no art. 2, item XV da IN-SLTI/MP 04 como [35]:

*"Documento que contém a descrição, a análise e o tratamento dos riscos e ameaças que possam vir a comprometer o sucesso em todas as fases da contratação".*

Segundo a norma, é responsabilidade da equipe que conduzirá o planejamento da contratação, executar todas as atividades relativas à gestão dos riscos da contratação de TI e produzir o artefato denominado análise de riscos. Tal artefato deve conter [35]:

1. A identificação dos principais riscos que possam comprometer o sucesso do processo de contratação e de gestão contratual;
2. A identificação dos principais riscos que possam fazer com que a solução de tecnologia da informação não alcance os resultados que atendam às necessidades da contratação;
3. A mensuração das probabilidades de ocorrência e dos danos potenciais relacionados a cada risco identificado;
4. A definição das ações previstas a serem tomadas para reduzir ou eliminar as chances de ocorrência dos eventos relacionado a cada risco;
5. A definição das ações de contingência a serem tomadas caso os eventos correspondentes aos riscos se concretizem; e
6. A definição dos responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência.

Em 2012 o TCU lançou o Guia de boas práticas em contratação de TI, que ofereceu aos órgãos da APF recomendações referentes ao planejamento das contratações de TI, baseadas na jurisprudência, em consonância com as leis e as melhores práticas do mercado, ajudando os gestores a evitar problemas amplamente conhecidos, incluindo sugestão de controles a riscos já identificados ao processo de contratação de TI [24].

Tal guia é composto por um banco de informações com 66 riscos comumente encontrados nas contratações de TI encontradas na APF. Alguns desses riscos, como os descritos abaixo, também são encontradas nos trabalhos dos autores Cruz et. al. (2011) e Wright (2004) [19]:

- Riscos de dependência de fornecedor;
- Riscos com a segurança das informações de negócio;
- Descontinuidade tecnológica;
- Dificuldade com a definição do escopo dos serviços;
- Falta de compreensão do negócio pelos contratados;
- Dificuldade em manter a qualidade dos serviços;

- Perda do domínio do conhecimento de negócio;
- Perda do controle da informação de negócio;
- Perda de política interna de incentivo aos servidores;
- Disputas entre equipes internas e de terceiros;
- Problemas com diferenças de rendimentos;
- Dificuldade em manter os padrões internos;
- Risco de desequilíbrio financeiro do contrato; e
- Perda de controle dos custos do contrato.

Todos esses riscos afetam o valor que a TI gera para o negócio da organização, e podem prejudicar, além do processo de contratação de serviços de tecnologia da informação para organizações públicas, a própria missão institucional pública que se destina. Isso demonstra como as contratações de TI merecem atenção especial e como os riscos devem ser adequadamente dirigidos, controlados e monitorados através de um modelo que apresente um conjunto de boas práticas, levando em conta aspectos importantes, como agregação de valor, atendimento das disposições legais e dos princípios básicos da Administração Pública [74].

## 2.4 Modelos de Gestão de Riscos

A gestão de risco em projetos, é atualmente, um tema de bastante interesse para pesquisadores e profissionais que trabalham na área de gerenciamento de projetos. Diversos modelos são apresentados na literatura com o objetivo de colaborar para o aprofundamento do conhecimento nessa disciplina [70]. Os modelos propostos por Boehm (1993) [10], Fairley (1994) [42], Kliem et. al. (1997) [57] e Gray (1998) [48] demonstram a importância do controle dos riscos para o sucesso dos projetos nas organizações. Outros modelos, como dos autores Hu (2013) [51] e Marcelino (2014) [63] destacam a necessidade do contínuo esforço das ações de controles nos projetos para evitar consequências negativas, inclusive financeira, para as organizações.

As metodologias de gestão de risco propostas, em qualquer dos modelos adotados nos setores público ou privado, nacionais e internacionais, descrevem uma abordagem que privilegia o alcance de resultados e que possibilita a execução em diversos níveis da organização, abrangendo processos específicos ou atingindo todas as atividades de uma empresa [68]. O Quadro 2.1 descreve as metodologias que serão descritas nesta seção como base conceitual para composição do modelo proposto. Estes modelos foram escolhidos por

sua atualidade e por demonstrarem a possibilidade de adesão ao tema de contratações de TI:

**Quadro 2.1:** Modelos de gestão de riscos. (Fonte: Elaboração própria)

| Modelo | Nº de processos | Fonte |
|---|---|---|
| ***Institute Risk Management - IRM* (2002)** | 7 processos | [65] |
| **Chapman e Ward (2003)** | 6 processos | [15] |
| ***The Orange Book* (2004)** | 6 processos | [80] |
| **ISO31000 (2009)** | 6 processos | [54] |
| **COBIT5 (2012)** | 5 processos | [5] |
| **PMBOK (2013)** | 5 processos | [67] |

Os modelos apresentam similaridades, seja pela quantidade ou disposição de seus processos. Os processos de identificação, análise e avaliação, além de alguma abordagem para o tratamento dos riscos, são descritos em todos modelos. Além disso, os modelos demonstrados pelo IRM, Chapman e Ward, *The Orange Book*, ISO 31000 e o PMBOK demonstram importância para a comunicação e aprendizado constante durante o processo de gestão de riscos ao estabelecer atividades específicas para esta etapa, enquanto o COBIT não reserva um processo específico para a comunicação da gestão de riscos, apesar de referenciá-lo no modelo. Nas seções a seguir os modelos selecionados serão apresentados em detalhes e, em seguida, avaliados.

### 2.4.1 Modelo de Gestão de Riscos Segundo o *Institute Risk Management*

O *Institute Risk Management (IRM)* afirma que o processo de gerenciamento de riscos deve ser padronizado para todos os projetos da organização, com a garantia de que terminologias, tarefas e os objetivos para gerenciamento de riscos estejam claramente definidos. Para o IRM, o gerenciamento de riscos não deve ser apenas para corporações ou organizações públicas, mas para qualquer atividade, de curto ou longo prazo [65]. O modelo proposto pelo IRM é composto por 7 (sete) etapas, como ilustra a Figura 2.1:

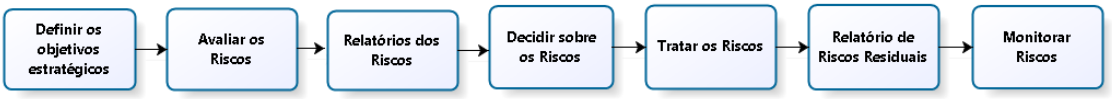


**Figura 2.1:** Modelo de gestão de riscos proposto pelo IRM. (Fonte: Adaptado de [65] ).

De acordo com o IRM, a partir do levantamento dos objetivos estratégicos da organização, define-se a avaliação dos riscos contendo a identificação, análise e estimativa dos riscos. Após a etapa de avaliação dos riscos concluída, gera-se um relatório de riscos que será base para os processos seguintes: decisão sobre os riscos, tratamento dos riscos, relatório de riscos residuais e monitoração dos riscos. O núcleo principal da gestão de riscos da metodologia proposta pelo IRM encontra-se dentro da etapa avaliação de riscos, onde estão os principais processos de identificação, descrição, estimativa e avaliação dos riscos [65].

O IRM descreve que a gestão de riscos tem que ser atenta não apenas ao contexto da própria atividade, mas principalmente em relação aos interessados e afetados do negócio. Além disso, destaca a importância da documentação e adaptabilidade do modelo à realidade de cada organização, recomendando a medição constante do processo para melhoria do modelo [65].

### 2.4.2 Modelo de Gestão de Riscos Segundo Chapman e Ward

O modelo proposto fornece uma estrutura para integrar o gerenciamento de riscos na gestão de projetos. Os autores afirmam que o gerenciamento de riscos é uma tarefa fundamental para os gerentes de projetos em qualquer projeto e que a metodologia proposta contribui para uma gestão de riscos sistemática com métodos e técnicas detalhadas [15]. O processo proposto pelos autores apresenta 6 etapas descritas na Figura 2.2:

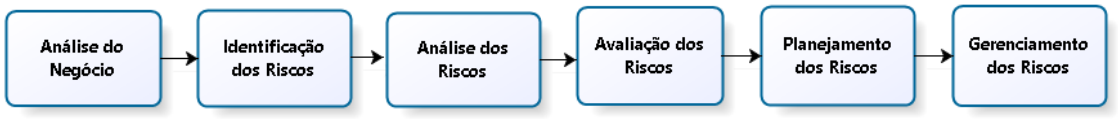


**Figura 2.2:** Modelo de gestão de riscos proposto por Chapman e Ward. (Fonte: Adaptado de [15] ).

A abordagem para a implementação do gerenciamento de riscos é apresentada contendo as etapas de análise do negócio, identificação, análise, avaliação, planejamento e gerenciamento dos riscos, o que, segundo os autores, segue a linha da maioria dos guias publicados sobre o tema de gerenciamento de riscos nos últimos 10 anos, embora algumas etapas possam ter rótulos diferentes. O modelo dispõe de atividades de planejamento e gerenciamento de riscos que catalisam esforços para definição de metas, ações, insumos, saídas, controles, mecanismos e atividades necessárias para compor a gestão de riscos em uma organização [15].

O destaque do modelo está na apresentação do processo chamado gerenciamento dos riscos que demonstra a preocupação de que a gestão de riscos esteja diretamente ligada

aos objetivos estratégicos da organização. O processo de gestão de riscos deve refletir diretamente nos resultados e nas ações globais da empresa. Para o modelo, a gestão de riscos é estratégica e deve grande importância para os gestores [15].

### 2.4.3 Modelo de Gestão de Riscos Segundo o *The Orange Book*

A edição do *The Orange Book*, foi publicada em 2004 pelo *HM Treasury*, órgão governamental responsável pelo tesouro ou finanças do Reino Unido, com o objetivo de fornecer orientações para o desenvolvimento de um quadro estratégico de gerenciamento de riscos para as organizações públicas daquele país. O guia provê um modelo de gestão de riscos que auxilia no desenvolvimento de uma política institucional, além de ser aplicável em diversos níveis, desde a organização como um todo, até projetos ou operações. O modelo proposto pelo documento é amplamente utilizado na matéria de gestão de riscos em ambientes governamentais [80]. A Figura 2.3 apresenta o ciclo proposto pelo modelo:

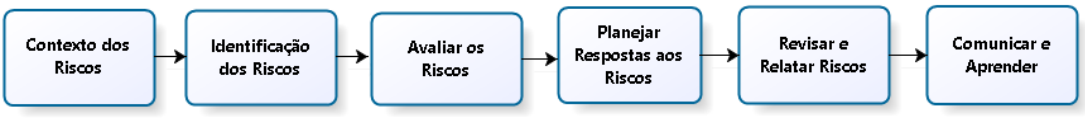


**Figura 2.3:** Modelo de gestão de riscos proposto por *The Orange Book*. (Fonte: Adaptado de [80]).

Entre os aspectos realçados no modelo, está a necessidade de comunicação, revisão e melhoria contínua do processo implantado. Além disso, enfatiza a necessidade da gestão de riscos considerar os relacionamentos de interdependência que a organização mantém com outras instituições, mapeando todos os riscos necessários envolvidos [80].

O modelo se apresenta bastante útil para aquelas instituições públicas que são iniciantes no gerenciamento de riscos, utilizando-o como documento introdutório que fornece boa base para o treinamento das organizações em gestão de riscos [80].

### 2.4.4 Modelo de Gestão de Riscos Segundo a ISO31000

A NBR ISO 31000 (2009) é considerada uma das principais referências no âmbito da gestão de riscos. A norma propõe que o processo de gestão de riscos seja parte integrante da gestão corporativa, incorporado na cultura e nas práticas da organização e que seja adaptado aos processos de negócio. A norma tem por finalidade ajudar a organização a aumentar a probabilidade de atingir seus objetivos, melhorar sua governança e estabelecer base confiável para a tomada de decisões [53]. A Figura 2.4 a seguir sintetiza o processo de gestão de riscos preconizado pela ISO:

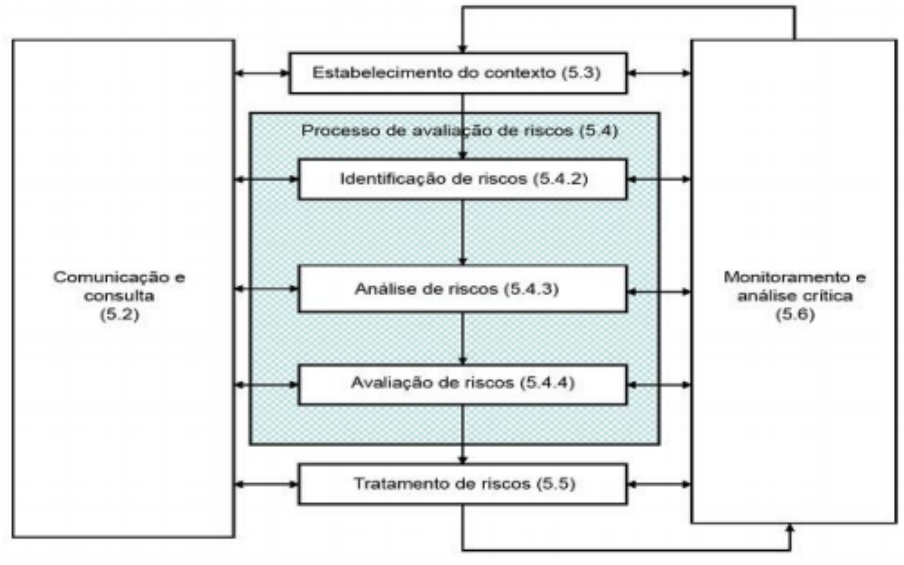


**Figura 2.4:** Modelo de gestão de riscos proposto pela ISO31000. (Fonte: [54]).

O modelo apresentado pela norma, tem como elementos essenciais, a necessidade de definição das responsabilidades pela gestão de riscos. Sem ela o conhecimento do gerenciamento do risco não é incorporado nos processos de negócio e não se desenvolve uma cultura de riscos na organização. No processo de estabelecimento do contexto, recomenda a apresentação dos objetivos organizacionais, e como estes são influenciados por fatores internos (como o planejamento estratégico de recursos e capacidades), e externos (como a análise de fatores como o ambiente cultural, político e econômico relacionado à instituição). Além disso, a NBR ISO 31000 ressalta a importância da comunicação sobre o risco, compreendendo a capacidade de melhoria contínua na gestão dos riscos [53].

O processo descrito pela ISO mantém semelhança com as principais normas que a antecederam, como a norma NBR ISO 27005 de 2008. As maiores novidades estão por conta da definição do conceito de risco e a explicitação de onze princípios para a gestão de riscos, bem como a apresentação dos cinco atributos para aprimorar a gestão de riscos. A norma se aplica a diversas áreas como: riscos financeiros, de projetos, segurança da informação e segurança empresarial [53].

### 2.4.5 Modelo de Gestão de Riscos Segundo o COBIT

O *Control Objectives For Information and Relatet Technology (COBIT)* é um modelo para a governança e gestão de TI, com sua edição atual, o Cobit 5, publicada em 2012. Ele propõe-se a servir como um modelo completo para a governança e a gestão corporativa de TI, em conformidade com as melhores práticas internacionais, com vistas a apoiar a alta direção e demais gestores na definição e no alcance de objetivos de negócio relacionados

com TI. O COBIT 5 publicou também o guia *"COBIT 5 for Risk"*, o qual descreve com maior profundidade práticas e métodos para auxiliar no processo de gestão de riscos de TI como um todo, e especialmente nas atividades relacionadas com a análise, avaliação e resposta a riscos. Esse guia também destaca a importância de uma perspectiva denominada função de riscos, que envolve a instituição de uma política e uma estrutura organizacional responsável por implantar e fomentar o processo de gestão de riscos de TI. A Figura 2.5, apresenta o modelo proposto pelo COBIT 5:

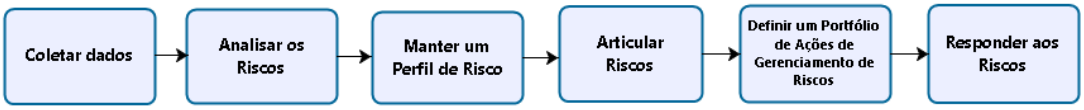


**Figura 2.5:** Modelo de gestão de riscos proposto pelo COBIT. (Fonte: Adaptado de [5]).

A metodologia para análise, identificação e tratamento dos riscos parte do levantamento de cenários de risco, que devem ser catalogados num universo de riscos. Os cenários são submetidos a análise, na qual se consideram os chamados fatores de riscos (ambiente externo e forças e fraquezas do ambiente interno). Na etapa de análise ponderam-se a probabilidade e as consequências, sendo que, para estas são sugeridos alguns tipos de impactos a considerar, como: não alcance de objetivos estratégicos, financeiros, legais/regulatórios, imagem/reputação e operacionais/produtividade. O guia destaca a importância de existirem critérios definidos pela alta direção (apetite de risco e tolerância a riscos) para subsidiar a decisão quanto à adoção de ações de mitigação [5].

O COBIT5 também reforça a necessidade de existirem critérios orientadores da gestão de riscos e o acompanhamento da alta direção sobre os resultados alcançados, preferencialmente no escopo de um processo de gestão institucional. Embora o COBIT5 seja voltado para a governança de TI, o modelo de gestão de riscos descrito pelo guia demonstra conformidade com as atividades dos demais modelos analisados [5].

### 2.4.6 Modelo de Gestão de Riscos Segundo o PMBOK

O *Project Management Body of Knowledge (PMBOK)* em sua 5º edição, é um guia composto por um conjunto de práticas para a gestão de projetos. O guia fornece uma gama de habilidades, ferramentas e técnicas que podem aumentar as chances de sucesso dos projetos. O PMBOK apresenta uma disciplina específica para o gerenciamento de riscos, especialmente elaborada para projetos, que detalham processos para aumentar a probabilidade de sucesso dos projetos e reduzir a probabilidade e o impacto dos eventos negativos no projeto [67]. A Figura 2.6 destaca os processos propostos pelo PMBOK:

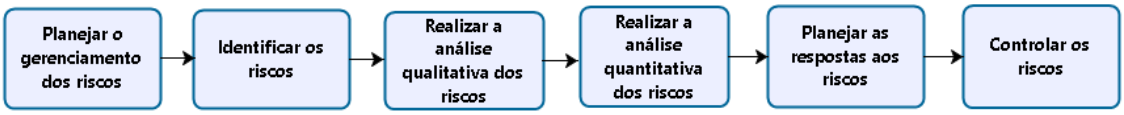


**Figura 2.6:** Modelo de gestão de riscos proposto pelo PMBOK. (Fonte: Adaptado de [67]).

No modelo de gerenciamento de riscos proposto pelo PMBOK, cada etapa é descrita com suas respectivas entradas, possíveis técnicas e ferramentas e as saídas esperadas, facilitando a implementação prática da metodologia. Para o modelo, a identificação dos riscos é um processo iterativo que deve durar durante todo o ciclo de vida do projeto. Além disso, propõe duas abordagens para análise dos riscos, uma qualitativa que prioriza a avaliação da probabilidade e impacto dos riscos, e outra quantitativa, que atribui uma classificação numérica para avaliar os efeitos dos riscos aos objetivos do projeto. A parte final do modelo propõe um planejamento adequado de resposta aos riscos com o contínuo monitoramento e controle de novos riscos, avaliando a eficácia do processo de gerenciamento de riscos [67].

O PMBOK ainda estabelece que a atitude das organizações em relação aos riscos pode ser influenciada por inúmero de fatores, como o grau de incerteza que uma entidade está disposta a aceitar (chamado de apetite de risco), o grau ou quantidade de riscos que a organização quer tolerar (chamado tolerância a riscos) e o limite ou impacto pelo qual a empresa aceitará o risco (chamado limite de riscos). Por fim, o modelo destaca que a organização deve estar comprometida com uma abordagem proativa e consistente do gerenciamento dos riscos durante todo o projeto. Todos os níveis da organização devem identificar ativamente e buscar o gerenciamento eficaz dos riscos durante o ciclo de vida do projeto [67].

### 2.4.7 Avaliação dos Modelos de Gestão de Riscos

Diante dos modelos estudados, pode-se perceber que os processos envolvidos no gerenciamento dos riscos como identificação, análise, avaliação, tratamento e monitoramento são inerentes à maioria das metodologias de gestão de riscos, o que Aris et. al. (2008) chamaram de *"princípios para o gerenciamento de riscos"*. Para os autores, no processo de gestão de riscos, as etapas de identificação, análise, avaliação e tratamento dos riscos são consideradas essenciais e básicas para toda metodologia de gestão de riscos [4]. Com base na revisão de literatura foi elaborado um quadro comparativo dos modelos que estão relacionados ao contexto deste trabalho, de acordo com o Quadro 2.2:

**Quadro 2.2:** Comparativo dos Modelos de Gestão de Riscos. (Fonte: Adaptado de [27] )

| **Característica** | ***Institute Risk Management* (2002)** | **Chapman e Ward (2003)** | ***The Orange Book* (2004)** | **ISO31000 (2009)** | **COBIT5 (2012)** | **PMBOK (2013)** |
|---|---|---|---|---|---|---|
| Considera oportunidades além de riscos | Sim | Sim | Sim | Sim | Sim | Sim |
| Necessidade de instituir Política de Gestão de riscos | Sim | Sim | Sim | Sim | Sim | Sim |
| Declara que o processo de gestão de riscos é customizável | Sim | Sim | Sim | Sim | Sim | Sim |
| Encoraja buscar a melhoria contínua da gestão de riscos | Sim | Sim | Sim | Sim | Sim | Sim |
| Apresenta que a gestão de riscos deve estar na rotina dos processos e na cultura organizacional | Sim | Sim | Sim | Sim | Sim | Sim |
| Associação de riscos com objetivos | Sim | Sim | Sim | Sim | Sim | Sim |
| Alerta sobre necessidade de considerar o custo de tratamento de riscos | Sim | Sim | Sim | Sim | Parcialmente | Sim |
| Orienta para a necessidade de documentar as atividades de gestão de riscos | Parcialmente | Sim | Sim | Sim | Sim | Sim |

Apesar dos itens “Alerta sobre necessidade de considerar o custo de tratamento de riscos” e “Orienta para a necessidade de documentar as atividades de gestão de riscos” terem os modelos COBIT5 e IRM respectivamente como características parciais, as propostas apresentam tais atributos, mas de maneira indireta, não descritas de forma clara no modelo.

Além das características analisadas, os modelos também recomendam a definição dos critérios pelos quais serão avaliados os riscos, estimulam a embutir a gestão de riscos na rotina dos processos de trabalho e na cultura organizacional, recomendam a criar um banco de informações com os riscos registrados, declaram que os riscos devem ter proprietários responsáveis pela evolução do risco e indicam que a implementação da gestão de riscos não é garantia de total sucesso.

Todas essas ações demonstram que o gerenciamento de riscos deve ser explorado juntamente com outras boas práticas, como as de gerenciamento de projetos, para que as chances de insucesso nos projetos sejam reduzidas e os objetivos sejam alcançados [79]. O Quadro 2.3 indica a análise dos pontos positivos e pontos negativos de cada modelo estudado:

**Quadro 2.3:** Avaliação dos Modelos de Gestão de Riscos. (Fonte: Elaboração própria)

| **Modelo** | **Pontos Positivos** | **Pontos Negativos** |
|---|---|---|
| ***Institute Risk Management* (2002)** | Modelo bem documentado que serviu de base para metodologias mais modernas. Apresenta uma lista de técnicas e métodos que podem ser utilizados junto às etapas da metodologia. | Mais antigo dos métodos estudados. Falta de descrição detalhada das atividades a serem realizadas em cada etapa do modelo. |
| **Chapman e Ward (2003)** | Modelo completo com etapas bem definidas e apresentadas de maneira detalhada. Para cada processo apresenta uma lista de entradas, saídas, limitações e técnicas que podem ser utilizadas. | Pode ser considerado complexo para pequenos projetos. Extensa documentação que pode desmotivar os interessados em iniciar a gestão de riscos em seus projetos. |

**Quadro 2.3**. Avaliação dos Modelos de Gestão de Riscos. (Fonte: Elaboração própria) **(Continuação)**

| Modelo | Pontos Positivos | Pontos Negativos |
|---|---|---|
| ***The Orange Book* (2004)** | Entende que a gestão de riscos é essencial para as organizações cumprirem seus objetivos. Aplicável às organizações públicas em diversos níveis, desde a organização como um todo, até projetos ou operações. | Modelo criado para instituições públicas, o que pode tornar o modelo não recomendado para outras esferas. |
| **ISO31000 (2009)** | Modelo iterativo de gestão de riscos que pode ser aplicado na estrutura organizacional em todos os níveis da organização, dentro de qualquer escopo e contexto. | Abordagem genérica para o tratamento de riscos. Para a aplicação de técnicas nos processos, devem ser utilizadas normas complementares. |
| **COBIT5 (2012)** | Reforça a necessidade de existirem critérios orientadores da gestão de riscos e monitoração da alta direção sobre os resultados alcançados, preferencialmente no escopo de um processo de gestão institucional. Fortemente relacionada à governança de TI e aos valores estratégicos. | Modelo complexo com muitas especializações e difícil aplicação prática. |
| **PMBOK (2013)** | Documentação completa e adaptável a todos modelos e tamanhos de organizações e projetos. Apresenta modelos qualitativos e quantitativos para análise dos riscos. Propõe entradas, saídas e técnicas para as atividades do projeto. | Aplicação do modelo pode ser de difícil adesão por sua complexidade. |

Diante de cada modelo de gestão de riscos, verificam-se características comuns entre todos. Para os modelos, a fase de identificação de riscos é a mais crítica pois encontra os problemas estratégicos e cuja ausência tem um grande impacto sobre os resultados do projeto [67]. A fase de análise dos modelos, avalia o estado de cada fator de risco identificado, e explora as relações entre os fatores de risco e a avaliação com base no impacto e razões de probabilidade [51].

Na etapa de avaliação do risco, as metodologias propõem critérios para se obter um valor quantitativo ou qualitativo dos riscos priorizando-os de acordo com sua gravidade e maior quantidade de exposição [73]. Após a avaliação e análise dos riscos, os modelos descrevem que o gerenciamento dos riscos deve estabelecer planos de ação com base nas recomendações para cada nível de risco, e priorizar as ações mais importantes que permitiriam aumentar a probabilidade de sucesso do projeto ou processo [63]. Deve-se coordenar os planos individuais para cada risco propondo implementação de ações [51]. Todo tratamento selecionado, deve ser documentado, monitorado, e analisado criticamente, e quando apropriado será dado tratamento adicional [22].

Os modelos elencados são considerados como referência e foram utilizados como base para a proposição da metodologia, objeto desse estudo, subsidiando assim a definição da estratégia de desenvolvimento da metodologia.

## 2.5 Técnicas para a Gestão de Riscos

As abordagens para a utilização de uma metodologia de gestão de riscos desenvolvem no ambiente institucional, um controle o qual, fornece maior garantia de que os objetivos organizacionais sejam alcançados dentro de um grau aceitável de risco [58]. Para a realização bem-sucedida do gerenciamento de riscos nos projetos é necessária a utilização de técnicas e ferramentas que maximizem todo processo [8].

A implementação da gestão de riscos de acordo com as boas práticas, princípios e técnicas, garante a entrega de melhores resultados para o devido tratamento, controle e redução da probabilidade de impacto dos riscos para as organizações [8].

Nos últimos anos, surgiu um grande interesse em melhorar a capacidade de lidar com o risco e a incerteza, especialmente com o seu impacto negativo nas organizações. Isto levou ao desenvolvimento e aplicação de ferramentas, técnicas, processos e metodologias de gestão de riscos. Estes fatores também resultaram em um número crescente de livros, artigos e conferências sendo dedicadas à gestão de risco e ao desenvolvimento de um certo número de padrões e boas práticas que contribuem para as organizações gerenciarem seus riscos da melhor maneira [69].

Diferentes percepções, atitudes e exigências levaram a uma variedade de definições e abordagens. Para os processos de gestão de risco, as técnicas de suporte foram amplamente desenvolvidas e implementadas tanto na literatura quanto na prática. Cada processo de gestão de risco requer ferramentas específicas a serem aplicadas. O Quadro 2.4 apresenta as técnicas que podem ser utilizadas nas diferentes fases da gestão de risco, de acordo com a ISO31010, e os autores que discorreram sobre o assunto:

**Quadro 2.4:** Técnicas para gestão de riscos. (Fonte: Elaboração própria)

| **Técnica** | **Identificação** | **Análise** | **Avaliação** |
|---|---|---|---|
| Análise crítica de modos de falha e efeito (FMECA) | [11] | [11] | [11] |
| Análise da confiabilidade humana | [61] | [61] | [61] |
| Análise de árvore de eventos | [64], [67] | [64], [67] | [64], [67] |
| Análise de árvore de falhas | —— | [40], [53] | [40], [53] |
| Análise de causa e efeito | [67], [53] | [67], [53] | —— |
| Análise de causa-raiz | —— | [71], [53] | [71], [53] |
| Análise de cenários | [53] | [53] | [53] |
| Análise de custo/benefício | [53] | [53] | [53] |
| Análise de Markov | —— | [67], [53], [15] | —— |
| Análise de modos de falha e efeito (FMEA) | [11], [67], [53], [15] | [11], [67], [53], [15] | [11], [67], [53], [15] |
| Análise do valor monetário esperado | —— | [67], [53] | [67], [53] |
| Análise preliminar de perigos | [2] | —— | —— |
| Análise sensitiva | —— | [15], [53] | —— |
| Análise SWOT | [41], [67], [53], [15] | [41], [67], [53], [15] | [41], [67], [53], [15] |
| Árvore de decisão | —— | [62], [53], [15] | [62], [53], [15] |

**Quadro 2.4**. Técnicas para gestão de riscos. (Fonte: Elaboração própria) **(Continuação)**

| **Técnica** | **Identificação** | **Análise** | **Avaliação** |
|---|---|---|---|
| Brainstorming | [67], [53], [15] | —— | —— |
| Delphi | [67],[15] | —— | —— |
| Entrevistas estruturadas ou semi-estruturadas | [53] | —— | —— |
| Estudo de perigos e operabilidade (HAZOP) | [56], [15] | [56], [15] | —— |
| Gráfico de fator casual de eventos | —— | [64] | [64] |
| Índice de risco / Análise de probabilidade e impacto / Ranking de riscos | [67], [53] | [67], [53] | [67], [53] |
| Listas de verificação (checklists) | [59],[67],[15] | —— | —— |
| Lógica Fuzzy | —— | [7] | [7] |
| Matriz analítica de riscos | —— | —— | [50] |
| Matriz Probabilidade/Consequência | [67], [53], [15] | [67], [53], [15] | [67], [53], [15] |
| Opinião especializada | [67] | [67] | [67] |
| Relatórios de incidentes | [81] | [81] | [81] |
| Técnica "5 por quês- 5 Whys | [64],[53] | [64],[53] | [64],[53] |
| Técnica Análise "E se- What-If | [64],[53] | [64],[53] | [64],[53] |
| Técnica estruturada "E se"(SWIFT) | [64],[53] | [64],[53] | [64],[53] |

As diversas técnicas existem na literatura para auxiliar na extração das informações e organizá-las para aumentar o conhecimento do risco. Cada etapa do processo de gestão de riscos implica em um nível de informação e detalhe, exigindo assim, técnicas adequadas, muitas vezes relacionadas entre si [12]. A fim de identificar os aspectos relevantes para se levar em conta ao escolher entre as técnicas de gestão dos riscos dos projetos, é amplamente comprovado e aceito que nenhuma técnica de gestão de riscos se adapta à todas as fases do processo e cada técnica dá seus melhores resultados se aplicada a uma ou poucas fases. Dessa maneira, a gestão dos riscos deve ser definida no contexto da sua aplicação [67].

A maneira como cada organização deve selecionar as técnicas para seu processo de

gestão de riscos deve seguir uma adequação com os objetivos e escopo do projeto. A NBR ISO 31010 (2009) estabelece que a escolha das técnicas deve seguir os seguintes princípios [53]:

- Convém que as técnicas sejam justificáveis e apropriadas à situação da organização em questão;
- Convém que a técnica selecionada proporcione resultados que ampliem o entendimento da natureza do risco e de como ele pode ser tratado;
- Convém que a técnica seja de uma forma rastreável, repetível e verificável;
- Os objetivos da gestão de riscos terão influência direta sobre as técnicas utilizadas;
- Um alto nível de detalhe é necessário para tomar uma boa decisão, em outros um entendimento mais geral é suficiente;
- A técnica selecionada deve estar de acordo com o tipo de riscos que estão sendo analisados;
- Convém que a decisão sobre a profundidade em que a gestão de riscos é conduzida reflita a percepção inicial das consequências;
- O grau de conhecimento especializado, recursos humanos e outros recursos necessários. Um método simples e bem feito pode fornecer melhores resultados do que um processo mais sofisticado e mal feito, contando que atenda aos objetivos e o escopo da gestão de riscos. O esforço aplicado à gestão de riscos está intimamente ligado ao nível potencial dos riscos analisados;
- Disponibilidade de informações e dados. Algumas técnicas requerem mais informações e dados que outras;
- A necessidade de modificação ou atualização do processo de gestão de riscos. Durante o processo de gestão de riscos algumas técnicas podem se tornar necessárias, enquanto outras podem ser descontinuadas;
- A técnica selecionada deve estar em conformidade com quaisquer requisitos regulatórios e contratuais.

Outros fatores podem ser considerados para a seleção de uma abordagem em gestão de riscos, como a natureza e o grau de incerteza, a quantidade, qualidade e a confiabilidade das informações de riscos disponíveis [53]. O PMI (2013) recomenda considerar a maturidade de conhecimento sobre risco do pessoal da organização que realiza a gestão de riscos ao selecionar técnicas de gestão de risco a fim de assegurar que a abordagem

adotada seja adequada às pessoas que irão aplicá-la e analisar seus resultados. A gestão de riscos pode ser aplicada a todos os estágios de vida do projeto e pode ter diferentes níveis de detalhe, a partir da técnica selecionada [67].

A capacidade para orientar a escolha das técnicas que devem ser aplicadas em diferentes contextos, dependem tanto do próprio projeto como da maturidade em relação ao risco da organização que a realiza, que é, por sua vez, uma função da quantidade de informações disponíveis. No caso em estudo, a proposta de solução será justamente a aglutinação de técnicas escolhidas em um modelo de gestão de risco elaborado para as contratações de TI da Funasa.

## 2.6 Governança de TI

A Governança de TI é a estrutura das relações e processos para dirigir e controlar os recursos de TI de modo a atingir os objetivos da organização, gerando um equilíbrio entre risco e retorno sobre recursos de TI e seus processos [60].

O tema governança de TI está em foco atualmente nas discussões sobre a racionalização e modernização da prestação de serviços públicos de qualidade [39]. Bernroider e Ivanov (2011) afirmam que a implantação da governança em TI contribui para garantir que a TI suporte os objetivos de negócios, além de otimizar os investimentos em TI e propiciar que papéis e responsabilidades em toda a organização sejam adequadamente desempenhados [9].

Nesse sentido, a contratação de serviços de TI tem papel importante na estratégia organizacional, onde há muitos riscos que podem frustrar seus resultados e impactar negativamente a governança de TI [9]. A norma ABNT NBR ISO 38500 (2009) também reconhece a importância das aquisições de TI ao citá-la dentro do universo de Governança de TI. Na norma são previstos seis princípios que devem nortear a boa governança de TI: responsabilidade, estratégia, aquisição, desempenho, conformidade e comportamento humano [1].

No setor público brasileiro, há muito tempo, as organizações reconhecem a importância da efetiva Governança de TI [52]. A busca por governança efetiva deixou de ser uma simples recomendação dos órgãos de controle, para se tornar uma imposição, para que os serviços prestados à sociedade sejam de melhor qualidade e estejam em conformidade com a legislação vigente, gerando importante meio para redução de gastos, transparência das ações e controle institucional [28].

Desde 2010 o Tribunal de Contas da União (TCU) tem aplicado questionários para obtenção do perfil governança de TI dos órgãos da APF. Do questionário verificam-se perguntas relacionadas ao planejamento de TI, processos de gestão, resultados, liderança

e contratações de TI. A partir das respostas, foi criado o iGovTI, conhecido como índice de governança de TI. Do resultado da última avaliação ainda surpreende que 16% das organizações não possuam processo de planejamento institucional e 25% não adotam processo de planejamento de TI, ou seja, há um risco elevado de que os projetos e atividades executados pela área de TI não estejam alinhados com as prioridades da instituição [25].

Diante da importância da governança de TI na aquisição de bens e serviços de TI para o setor público brasileiro, e diante de inúmeras auditorias realizadas que indicam deficiências na gestão da TI (acórdãos do TCU números 1.521/2003, 2.094/2004, 786/2006, 1.480/2007, 1.603/2008, 1.215/2009, 1.233/2012, 228/2015, 916/2015) é necessário que existam cada vez mais abordagens de aperfeiçoamento da gestão pública em relação as contratações de bens e serviços de TI.

## 2.7 Contratação de TI na APF

As contratações de TI representam um gasto anual médio, na esfera federal, que gira em torno de R$12,5 bilhões. Dessa maneira, exigem mecanismos de controle específicos que reduzam a probabilidade de prejuízos e incorreta aplicação desses valores.

O TCU tem atuado fortemente no diagnóstico da situação de TI na APF avaliando a situação dos órgãos quanto ao emprego dos recursos públicos, principalmente referente às contratações de TI, isto tem gerado um aumento na frequência de acórdãos e decisões relacionados ao assunto [19].

Os resultados do último ciclo de avaliação do iGovTI publicado em 2014 pelo TCU, avaliaram as práticas das contratações de TI, em uma análise de respostas de 355 órgãos e entidades da APF [21]. As questões referentes às contratações de TI existentes nas avaliações do TCU refletem a evolução da gestão das contratações de TI nos órgãos da APF, entretanto, demonstram um caminho de evolução necessário. A Figura 2.7 apresenta essa evolução:

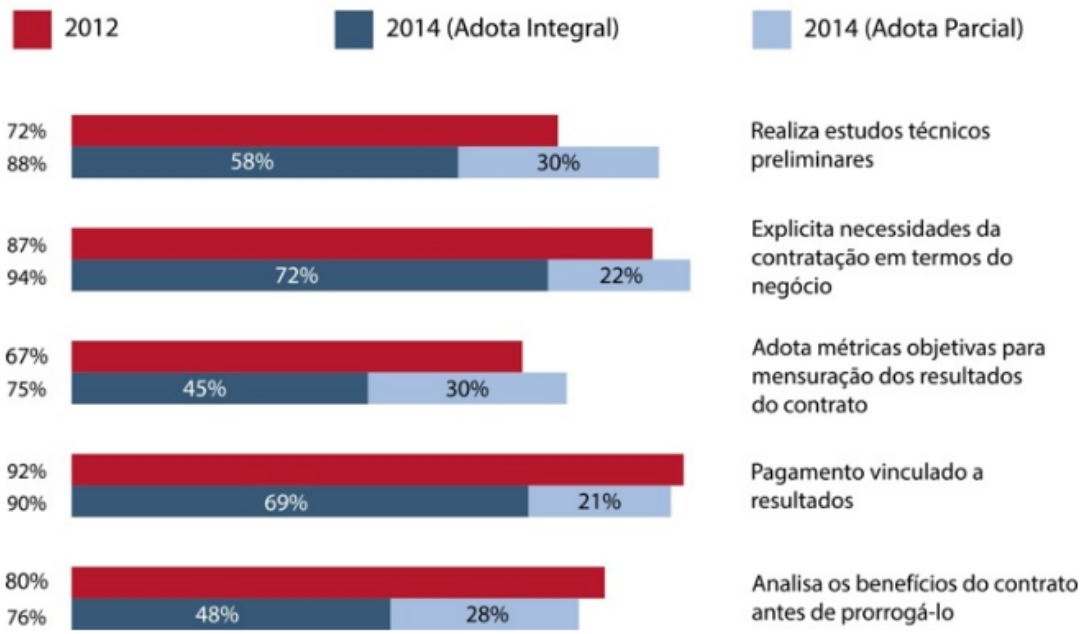


**Figura 2.7:** Evolução das práticas relativas à contratação de TI. (Fonte: [21]).

Observa-se que as instituições públicas evoluíram quanto à realização de estudos preliminares. Até 2014 72% dos órgãos realizam estudos preliminares como base para as contratações de TI. Esse número aumentou para 88% em 2014. Outros pontos também apresentam crescimento de qualidade como a prática de explicitar necessidades da contratação em termos do negócio, que saiu de 87% de 2012 para 94% em 2014, também a adoção de métricas objetivas para mensuração dos resultados do contrato melhorou em 2012 de 67% para 75%. Dos números apresentados percebe-se uma melhoria na ação dos órgãos públicos, principalmente para o objetivo que as contratações se dão, que é o atendimento das necessidades do negócio. Contudo, deve-se observar que as práticas para as contratações de TI estão normatizadas, o que faz com que os órgãos sejam deliberados a cumprirem em sua totalidade as práticas avaliadas, o que na prática deveria trazer um número maior de órgãos em conformidade, o que não se verifica na avaliação. [21]

Outros pontos avaliados no iGovTI 2014, têm interessante riqueza de informação que devem ser analisados, de acordo com a Figura 2.8:

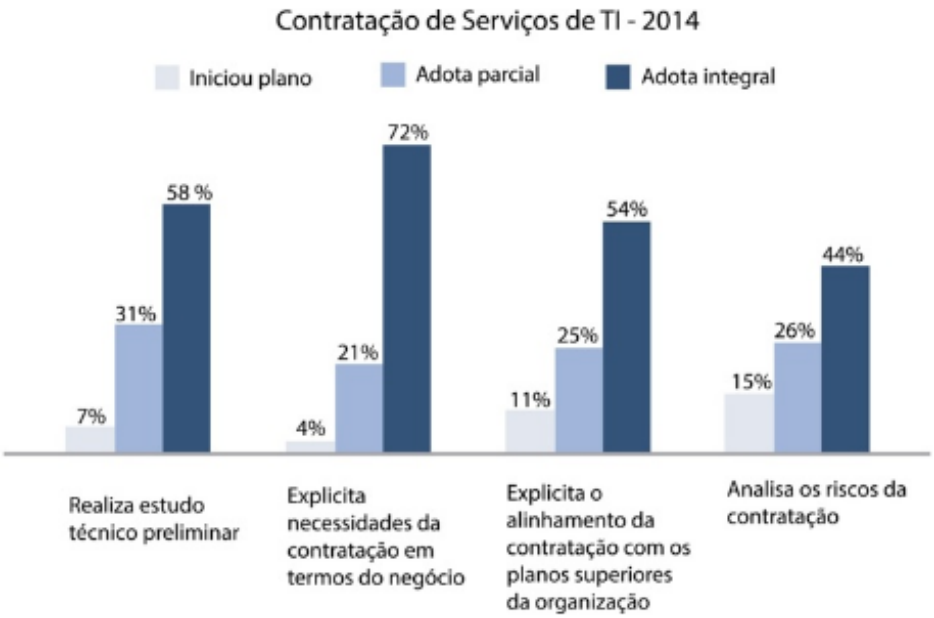


**Figura 2.8:** Contratação de serviços de TI 2014. (Fonte: [25]).

O relatório apresentado pelo TCU descreve que em relação aos estudos preliminares para avaliar a viabilidade da contratação de serviços de TI, verifica-se que 89% das organizações participantes declararam adotar essa prática (31% parcialmente e 58% integralmente). O desenvolvimento dos estudos preliminares para as contratações de TI, são de cumprimento obrigatório para os órgãos e entidades públicas, dessa maneira, esse percentual não pode ser considerado totalmente satisfatório, tendo em vista que 11% das organizações correm sérios riscos de causarem prejuízo aos cofres públicos com contratações inviáveis [25].

Em relação à vinculação da contratação com os objetivos de negócio da organização, o relatório do TCU destaca que, 93% dos participantes (21% parcialmente e 72% integralmente) afirmam relacionar as necessidades de negócio com o que se pretende atender com a contratação. Além disso, apenas 73% (31% parcialmente e 42% integralmente) das instituições públicas relacionam os indicadores dos benefícios do negócio que serão alcançados com a contratação de TI e 79% (25% parcialmente e 54% integralmente) demonstram o alinhamento entre a contratação e os planos estratégico institucional e de TI vigentes. Esse item demonstra que algumas organizações ainda realizam contratações de TI sem que haja um claro entendimento de como elas contribuirão para o negócio [25].

Quanto à realização da gestão de riscos nas contratações de TI, a pesquisa apresenta que 70% dos participantes declararam realizar análise dos riscos que possam afetar o sucesso da contratação (26% parcialmente e 44% integralmente). Fica claro que, para o TCU, parte das organizações (30%) ainda depende da sorte para alcançar os resultados

esperados com as contratações de TI [25].

É importante ressaltar que os pontos avaliados são obrigatórios e devem compor todas as contratações de TI, ainda sim, uma boa quantidade de órgãos públicos tardam a adotá-los, causando grande prejuízo ao governo seja pela não conclusão das contratações de TI, seja pela conclusão com aquisição de produtos e serviços de má qualidade. O resultado revela que uma parcela das organizações públicas pode estar incorrendo em irregularidades quando da realização de suas contratações de TI, com grandes chances de impactos nos programas e projetos governamentais [25].

A avaliação da gestão dos riscos que afetam o sucesso das contratações de TI, demonstra que apenas 44% dos órgãos gerenciam integralmente os riscos e que boa parte das contratações de TI da APF está exposta a riscos que podem impactar diretamente os objetivos esperados e o serviço prestado à sociedade. Isto demonstra o caminho a perseguir pelas instituições públicas para a melhoria de qualidade de seus processos [21]. Neste sentido, o relatório do TCU destaca a importância da formalização do processo de contratação de TI para a padronização das atividades, evitando condutas que coloquem em risco a regularidade e o alcance dos objetivos do futuro contrato [25].

O processo de contratação de TI pela APF tem evoluído, o relatório do TCU apresenta essa evolução. Ainda assim, outros pontos merecem atenção especial, como a gestão dos riscos. A legislação deve favorecer aos gestores públicos um ambiente de melhoria dos processos e produtos adquiridos, trazendo conformidade aos atos e inserindo as organizações nas melhores práticas utilizadas pelas instituições.

### 2.7.1 Normas de contratação de TI

A norma NBR ISO 38500 (2009) prevê princípios para conduzir a governança de TI: responsabilidade, estratégia, aquisição, desempenho, conformidade e comportamento humano. Destaque para o princípio da conformidade, segundo o qual é necessário garantir que *"a TI cumpra com toda a legislação e regulamentos obrigatórios. As políticas e práticas são claramente definidas, implementadas e fiscalizadas"* [1]. A norma se alinha à Constituição Federal de 1988 que se rege por vários princípios, entre eles o da legalidade, no qual o administrador público deve pautar suas ações pela legislação e jurisprudência em vigor [43].

A legislação atual aplicável às contratações de TI na APF é bastante vasta, destacam-se alguns documentos que regulamentam o processo de trabalho de contratação de TI que serão vistos adiante num estudo histórico acerca do assunto, além do detalhamento da IN-SLTI/MP 04/2014, norma mais recente referente ao trabalho. O Quadro 2.5 apresenta cronologicamente as principais leis, normas, acórdãos relacionados às contratações de TI:

**Quadro 2.5:** Normas relacionadas com contratações de TI. (Fonte: Elaboração própria)

| **Norma/Ano** | **Data** | **Descrição** |
|---|---|---|
| Constituição Federal/1988 | 05/10/1988 | Estabelece a realização de licitação pública como a regra para as contratações públicas. |
| Lei nº 8.248/1991 | 23/10/1991 | Define o que são bens e serviços comuns de informática e automação. |
| Lei nº 8.666/1993 | 21/06/1993 | Norma geral aplicável a todas as esferas de poder da república brasileira. Institui as regras para licitações e contratos a serem realizados pela administração pública. |
| Dec. nº 1.048/1993 | 21/01/1994 | Regulamenta o SISP - Sistema de Recursos de Informação e Informática. Responsável pelo planejamento, coordenação, organização, operação, controle e supervisão dos recursos de informática. |
| Dec. nº 2.271/1997 | 07/07/1997 | Dispõe as atividades que são objeto de contratação por licitação, que poderão ser contratados atividades acessórias ou complementares aos assuntos de competência legal do órgão. As atividades de informática são consideradas objetos de contratação. |
| Lei nº 9.784/1999 | 29/01/1999 | Regula o processo administrativo no âmbito federal. Como a licitação é um procedimento administrativo composto por diversos atos, os dispositivos dessa lei devem ser observados pelo gestor público. |
| Dec. nº 3.555/2000 | 08/08/2000 | Define o pregão como modalidade de licitação para aquisição de bens e serviços comuns. |
| Dec. nº 3.931/2001 | 19/09/2001 | Define o Sistema de Registro de Preços - SRP, para registro formal de preços em relação a prestação de serviços comuns e aquisição de bens. |

**Quadro 2.5**. Normas relacionadas com contratações de TI. (Fonte: Elaboração própria)
**(Continuação)**

| **Norma/Ano** | **Data** | **Descrição** |
|---|---|---|
| Lei nº 10.520/2002 | 17/07/2002 | Regulamentação do decreto nº 3.555/2000 no qual instituiu a modalidade de licitação pregão para aquisição de bens e serviços comuns, podendo ser realizada na forma de pregão eletrônico, conferindo agilidade e ampliação das compras governamentais. |
| Acórdão do TCU nº 1.521/2003 | 08/10/2003 | Reforça a necessidade de planejamento para as contratações de TI. |
| Acórdão do TCU nº 1.558/2003 | 15/10/2003 | Avaliar a legalidade e a oportunidade das aquisições de bens e serviços de informática. Ausência de planejamento nas aquisições de bens e serviços de informática. |
| Acórdão do TCU nº 2.094/2004 | 15/12/2004 | Fiscalização quanto à legalidade e oportunidade das contratações e aquisições de bens e serviços de informática, planejamento deficiente do setor de informática. |
| Lei nº 11.077/2004 | 30/12/2004 | Dispõe sobre a capacitação e competitividade do setor de informática e recomenda o uso do pregão eletrônico para as licitações que a lei define. |
| Dec. nº 5.450/2005 | 31/05/2005 | Regulamenta o pregão na forma eletrônica, devendo ser utilizada obrigatoriamente para licitações. |
| Acórdão do TCU nº 786/2006 | 24/06/2006 | Fiscalização do TCU nas contratações de informática. Recomendou ao órgão central a elaboração de um modelo de licitação específico para as contratações de informática para a APF, promovendo a implementação nos diversos órgãos, mediante orientação normativa. |

**Quadro 2.5**. Normas relacionadas com contratações de TI. (Fonte: Elaboração própria)
**(Continuação)**

| **Norma/Ano** | **Data** | **Descrição** |
|---|---|---|
| Acórdão do TCU nº 1.480/2007 | 28/11/2007 | Definiu a expressão *solução de TI* para designar todo conjunto de bens e serviços relativos à contratação e à gestão de contratos de soluções de TI. |
| Instrução Normativa nº 02 MPOG/SLTI/2008 | 30/04/2008 | Disciplina as regras e diretrizes para a contratação de serviços continuados ou não. |
| Instrução Normativa nº 04 MPOG/SLTI/2008 | 20/05/2008 | Disciplina as regras e diretrizes para as contratações de serviços de TI pelos órgãos e entidades integrantes do SISP. |
| Acórdão do TCU nº 1.603/2008 | 13/08/2008 | Resultado do primeiro levantamento de governança de TI da APF, com diversos apontamentos de fragilidades nas estruturas de controle dos órgãos federais. |
| Acórdão do TCU nº 1.215/2009 | 10/12/2009 | Divulgação de um estudo acerca das contratações de TI, chamado *Quadro Referencial Normativo*, um modelo genérico de contratação de serviços de TI baseado na legislação, jurisprudência, doutrina e melhores práticas do mercado. |
| Dec. nº 7.174/2010 | 12/05/2010 | Estabelece exigências nas licitações públicas para TI exigindo elaboração de planejamento da contratação, incluindo projeto básico ou TR com as especificações do objeto a ser contratado. |
| Instrução Normativa nº 04 MPOG/SLTI/2010 | 16/11/2010 | Revoga a IN04 MPOG/SLTI/2008 e reorganiza os tópicos e etapas que devem ser cumpridas para as contratações de TI da APF. |
| Acórdão do TCU nº 1.233/2012 | 23/05/2012 | Estabelece entendimentos quanto ao planejamento estratégico de TI, controles internos, contratações de TI e ao uso do registro de preços para bens e serviços de TI. |
| Dec. nº 7.892/2013 | 23/01/2013 | Reformulação do Sistema de Registro de Preços (SRP). |

**Quadro 2.5**. Normas relacionadas com contratações de TI. (Fonte: Elaboração própria)
**(Continuação)**

| **Norma/Ano** | **Data** | **Descrição** |
|---|---|---|
| Dec. nº 7.903/2013 | 04/02/2013 | Estabelece margem de preferência em licitações federais de equipamentos de redes em comunicação. |
| Dec. nº 8.135/2013 | 04/11/2013 | Regulamenta a contratação de serviços de comunicação de dados que possam comprometer a segurança nacional. |
| Dec. nº 8.184, 8.186 e 8.194/2014 | 17/01/2014, 17/01/2014 e 12/02/2014 | Estabelece margem de preferência em licitações federais para bens e serviços de TI. |
| Instrução Normativa nº 04 MPOG/SLTI/2014 | 11/09/2014 | Revoga a IN04 MPOG/SLTI/2010 e simplificação do processo e obrigatoriedade explícita da existência e operação do Plano Diretor de Tecnologia da Informação (PDTI) para se proceder com as contratações de TI. |
| Acórdão do TCU nº 916/2015 | 22/04/2015 | Relatório de consolidação das auditorias realizadas com o objetivo de avaliar o processo de trabalho de gestão de contratos de Tecnologia da Informação - TI. |
| Acórdão do TCU nº 2.622/2015 | 21/10/2015 | Relatório de levantamento com o objetivo de sistematizar informações sobre a situação da governança e da gestão das aquisições em amostra de organizações da APF, a fim de identificar os pontos vulneráveis e induzir melhorias na área. |
| Portaria MP/STI nº 20 | 14/06/2016 | Orientações técnicas para as contratações de soluções de TI na APF auxiliando na elaboração de suas especificações técnicas. |
| Portaria MP/STI nº 40 | 14/09/2016 | Institui o plano de contratações de soluções de TI como ferramenta de planejamento a ser consolidada pelos órgãos integrantes SISP. |

A evolução dos normativos e documentos referentes às contratações de bens e soluções de TI tornaram mais robusto o processo de aquisição dos órgãos da APF, contudo, a legislação pública sobre contratações ainda se apresenta complexa para garantir um processo eficiente de contratação. O atual modelo de contratação de TI estabelecido pela então Secretaria de Logística e Tecnologia da Informação (SLTI), a IN-SLTI/MP 04/2014, tem importante destaque no cenário público federal, pois trouxe grande produtividade aos órgãos da APF por sua boa aderência nos órgãos, unificando os normativos em documento único, padronizando as ações e melhorando os resultados apresentados [19].

### 2.7.2 Instrução Normativa nº 04 MP/SLTI/2014

A Instrução Normativa nº 4/2014 (IN-SLTI/MP 04/2014) é considerada o principal marco regulatório para as contratações de TI no âmbito da APF, ela reúne a legislação que trata das contratações de TI em um único documento. Além disso, estabelece diretrizes, normatiza métodos, procedimentos e regulamenta matéria anteriormente disciplinada a fim de orientar os dirigentes e servidores envolvidos na contratação de produtos e serviços de tecnologia [35]. A IN-SLTI/MP 04/2014 apresenta um modelo de processo de trabalho com as etapas, responsabilidades dos envolvidos e artefatos que devem ser produzidos em cada etapa do modelo. Caracteriza-se, principalmente, por reduzir o número de artefatos da fase de planejamento da contratação, que existiam na norma anterior, IN-SLTI/MP 04/2010 [21].

A estrutura da norma provê mecanismos de governança para as contratações de TI desde o nível mais alto de gestão, como a obrigatoriedade de alinhamento com instrumentos de planejamento como o Plano Diretor de Tecnologia da Informação (PDTI), até o nível mais baixo no processo de contratação dos bens e serviços de TI, constituído das seguintes fases:

1. Planejamento da contratação;
2. Seleção do fornecedor; e
3. Gestão do contrato.

A fase planejamento da contratação observa a definição das responsabilidades dos envolvidos, identifica a necessidade da contratação considerando os objetivos estratégicos e as necessidades corporativas da instituição, bem como seu alinhamento com o PDTI. Essa fase tem início com o recebimento do Documento de Oficialização da Demanda (DOD), pela área de TI. Consiste nas seguintes etapas [35]:

1. Instituição da equipe de planejamento da contratação: será composta por integrante técnico, indicado pela área de TI, integrante administrativo, indicado pela área de

administração e integrante requisitante, indicado pelo setor solicitante da solução de TI a ser adquirida;

2. Estudo técnico preliminar da contratação: será realizado pelos integrantes nomeados com a missão de definir as especificações das necessidades de negócio e tecnológicas e dos requisitos necessários e suficientes à escolha da solução de tecnologia da informação;

3. Análise de riscos: permeia todas as etapas do planejamento da contratação com a gestão dos principais riscos que possam comprometer o sucesso dos processos de contratação e da gestão contratual e deve ser finalizada somente após o término dos demais processos que compõem o planejamento da contratação; e

4. Termo de referência ou projeto básico: elaborado pela equipe de planejamento a partir do estudo técnico preliminar.

A fase de seleção do fornecedor inicia com o encaminhamento do termo de referência à área de licitações, cabendo a respectiva área conduzir as etapas de seleção do fornecedor de com a lei nº 8666/1993 e demais normas. A área de TI irá apoiar tecnicamente o pregoeiro ou a comissão de licitação na resposta aos questionamentos e impugnações dos licitantes na análise das propostas apresentadas, sendo encerrada com a assinatura do contrato e a nomeação dos responsáveis pela fiscalização do contrato: gestor do contrato, fiscais técnico, requisitante e administrativo do contrato [19].

Por fim a fase de gestão contratual acompanha e garante a adequada prestação dos serviços e o fornecimento dos bens da solução de TI adquirida durante todo o período compactuado. É composto pelas seguintes etapas [35]:

1. Início do contrato: elaboração do plano de inserção da contratada com repasse de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens além da disponibilização da infraestrutura adequada, plano de fiscalização e realização das reuniões iniciais;

2. Encaminhamento formal de demandas: definição e especificação dos serviços a serem realizados ou bens a serem fornecidos, cronograma e responsáveis pelas demandas;

3. Monitoramento da execução: assinatura dos termos de recebimento provisório ou definitivo, avaliação da qualidade dos serviços, identificação de não conformidades nos termos contratuais e demais correções necessárias que sejam identificadas durante a execução contratual; e

4. Transição e encerramento contratual: manutenção dos recursos materiais e humanos necessários à continuidade do negócio, entrega das versões finais e documentação e transferência de conhecimento necessário para não interrupção dos serviços.

Após a publicação da IN-SLTI/MP 04, outros documentos também surgiram com objetivo de auxiliar os gestores na adoção da norma nos órgãos, como o Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação, versão 2.0 de setembro de 2014, da Secretaria de Tecnologia da Informação do Ministério do Planejamento, que descreve os processos, atividades e artefatos envolvidos, e também outro guia com o mesmo nome só que elaborado pelo TCU em 2012, com uma abordagem voltada aos riscos e controles para o planejamento da contratação.

No próximo capítulo é apresentado a metodologia científica com os métodos e as técnicas de pesquisa utilizadas para elaboração da proposta de metodologia de gestão de riscos para as contratações de TI da FUNASA.

# Capítulo 3

# Metodologia da Pesquisa

Este capítulo descreve a metodologia para a construção da proposta para apoiar o gerenciamento dos riscos no planejamento da contratação de TI da FUNASA.

## 3.1 Métodos de Pesquisa

O método de pesquisa deve descrever os procedimentos ordenados para a compreensão do instrumento de trabalho, selecionando os meios e os processos mais adequados para o alcance dos objetivos. Gil (2010) descreve que a pesquisa aplicada objetiva gerar conhecimentos dirigidos à solução de problemas específicos. Este tipo de pesquisa, visa à aplicação de suas descobertas para um problema reconhecido [47]. A Figura 3.1 demonstra os métodos de pesquisa aplicados à metodologia proposta:

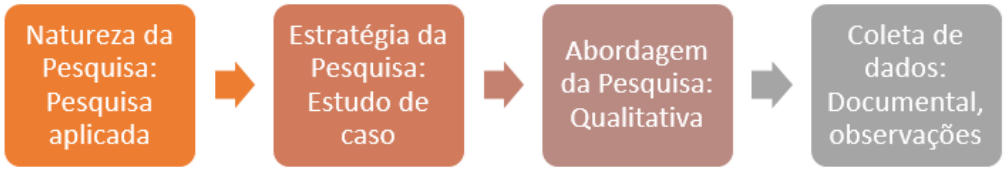


**Figura 3.1:** Métodos de pesquisa aplicados. (Fonte: Elaboração própria).

Esta pesquisa é aplicada pois a elaboração da metodologia proposta busca solucionar problemas reais encontrados pela FUNASA. Além disso, a pesquisa é exploratória, pois as especificidades do ambiente da FUNASA são características únicas, que não foram exaustivamente discutidas ou encontradas na APF, e visa trazer novas discussões sobre a contratação de serviços de TI, a partir da realidade diagnosticada na organização, juntamente com a adoção de técnicas, ferramentas e das boas práticas pesquisadas e já amplamente utilizadas [46].

Para Yin (2005) um estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos [84]. A estratégia da pesquisa é utilizar a FUNASA como estudo de caso, com a coleta dos dados sobre as contratações de TI, descrevendo a pesquisa documental elaborada a partir de materiais que não receberam tratamento analítico, como documentos, normas, relatórios de empresas e manuais [46]. Além disso, a coleta de dados da pesquisa considera a observação e a percepção direta e passiva do objeto de estudo. Nesta pesquisa serão realizadas pesquisas bibliográficas, análises do ambiente e observações.

## 3.2 Estruturação da Pesquisa

A solução proposta se refere à proposição de uma metodologia para gestão de riscos nas contratações de TI com a utilização de técnicas e ferramentas estudadas. O PMBOK (2013) descreve que uma metodologia define abordagens, ferramentas e fontes de dados que podem ser usadas para realizar o gerenciamento dos riscos no projeto [67]. A metodologia proposta está alinhada à Metodologia de Gestão de Riscos de Segurança da Informação do Ministério do Planejamento e às normas legais como a IN-SLTI/MP 04/2014 e à Instrução Normativa Conjunta nº 1, de 10 de maio de 2016, publicada pela Controladoria-Geral da União (CGU) e pelo Ministério do Planejamento, Orçamento e Gestão, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal [36]. Como base para o trabalho, foram realizadas pesquisas bibliográficas em material já elaborado, constituído principalmente de normas, livros e artigos científicos [46]. A Figura 3.2 representa a estrutura da pesquisa contemplando suas principais etapas.

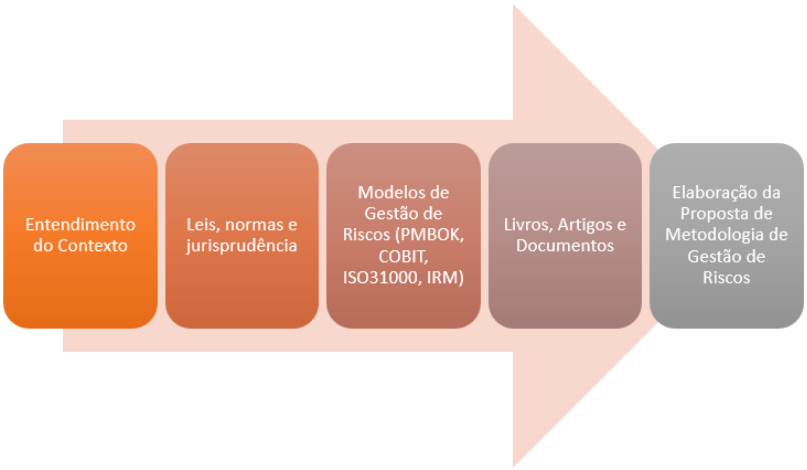


**Figura 3.2:** Estrutura da pesquisa. (Fonte: Elaboração própria).

Para o desenvolvimento da metodologia, buscou-se também o respaldo de padrões bem aceitos, como ABNT NBR ISO 31000 (2009), 31010 (2009), *The Institute of Risk Management* - IRM (2002), COBIT5, *The Orange Book* (2004) e o *Guide to the Project Management Body of Knowledge - PMBOK* (2013), que forneceram elementos para a definição da metodologia proposta. De acordo com a ISO 31000, o processo de gestão dos riscos deve estar integrado às melhores práticas, juntamente com a utilização de atividades e ferramentas que proporcionam um processo efetivo de controle e monitoração dos riscos envolvidos [54].

A presente proposta metodológica tem respaldo na norma complementar nº 04 do Gabinete de Segurança Institucional do Departamento de Segurança da Informação e Comunicações da Presidência da República que orienta os órgãos públicos a selecionarem uma metodologia de gestão de riscos mais apropriada ao escopo, no caso específico ao processo de contratações de TI, e de acordo com o contexto apresentado pelos órgãos.

A aplicação da metodologia de gestão de riscos para as contratações de TI na FUNASA pode ser apoiada por uma ferramenta computacional, muito embora a metodologia seja independente de qualquer ferramenta.

A metodologia é composta por um conjunto de processos descritos por seus papéis e responsabilidades. Os processos definem conjuntos de atividades estruturadas para que sejam atingidos os objetivos da gestão de riscos nas contratações de TI. Já as atividades são decompostas em um conjunto de tarefas bem definidas.

Cada etapa do processo deve ser medida em relação a metas específicas que refletem diretamente na contribuição final que deve trazer para a metodologia [16]. O processo da gestão de riscos das contratações de TI proposto está em conformidade com às atividades previstas no art. 13 da IN-SLTI/MP 04/2014 em conjunto com modelos estudados.

A partir do estudo da base conceitual e da metodologia de pesquisa descrita, o próximo capítulo descreve o estudo de caso com o contexto no qual está inserido a pesquisa, com uma análise da situação atual do objeto de estudo.

# Capítulo 4

# Análise da Situação Atual

Este capítulo descreve o estudo de caso na Fundação Nacional de Saúde (FUNASA), demonstrando o contexto em que está inserida a instituição e a motivação que inspirou a presente pesquisa.

## 4.1 Contexto Externo

A Fundação Nacional de Saúde (FUNASA), é um órgão executivo do Ministério da Saúde, responsável em promover a inclusão social por meio de ações de saneamento para prevenção e controle de doenças. Além disso, é responsável por formular e implementar ações de promoção e proteção à saúde relacionadas com as ações estabelecidas pelo Subsistema Nacional de Vigilância em Saúde Ambiental [44].

As ações da FUNASA de prevenção e controle de doenças se dão pela adequação das condições de saneamento básico em áreas como de assentamentos, remanescentes de quilombos e reservas extrativistas. Os investimentos da instituição visam intervir no meio ambiente, na infraestrutura dos municípios de até 50 mil habitantes, o que representa mais de 80% dos municípios brasileiros, melhorando as condições de vida de populações vulneráveis e prevenindo doenças [44].

A FUNASA possui larga experiência no apoio de projetos ligados à engenharia de saúde pública, auxiliando estados e municípios na melhoria de indicadores sanitários, epidemiológicos, ambientais e sociais. Tais indicadores impactam no controle e redução da mortalidade infantil e da incidência de doenças de veiculação hídrica ou causadas pela falta de saneamento básico e ambiental. As áreas de atuação da FUNASA são [44]:

1. Engenharia de Saúde Pública: nessa área, a FUNASA busca a construção e ampliação de sistemas de abastecimento de água e de esgotamento sanitário, implantação de melhorias sanitárias domiciliares, implantação, ampliação ou melhoria dos

sistemas de tratamento e destinação final de resíduos sólidos. Todas essas ações impactam aproximadamente, 35 milhões de pessoas no Brasil. Na área de engenharia de saúde pública, os projetos prioritários estão ligados à promoção, apoio técnico e financeiro ao controle de qualidade da água para consumo humano, o estímulo e financiamento de projetos de pesquisa em saneamento, e o apoio técnico a estados e municípios para a execução de projetos de saneamento, passando por estratégias de cooperação técnica. Com ações de saneamento básico, a FUNASA faz parte e colabora com o Sistema Único de Saúde (SUS);

2. Saúde Ambiental: nessa área, a FUNASA busca ações de planejamento, coordenação, supervisão e monitoria da execução das atividades relativas à formulação e implementação de ações de promoção e proteção à saúde ambiental, controle da qualidade de água para consumo humano proveniente de sistemas de abastecimento público e apoio ao desenvolvimento de estudos e pesquisas na área de saúde ambiental.

A FUNASA é uma fundação pública, instituída com base na Lei nº 8.029, de 12 de abril de 1990, que tem sua sede em Brasília/DF e conta com 26 unidades descentralizadas, uma em cada estado brasileiro, denominadas Superintendências Estaduais. Os contextos externos nas quais a FUNASA está inserida para atingir seus objetivos são:

1. Ambiente regulatório: as principais leis que regem à missão institucional da FUNASA são a Lei nº 8.080/1990 que dispõe sobre as condições para a promoção, proteção e recuperação da saúde e a Lei nº 8.029, de 12 de abril de 1990 que institui a FUNASA;

2. Meio ambiente: os investimentos da FUNASA interferem diretamente no meio ambiente, na infraestrutura dos municípios de até 50 mil habitantes, para melhorar as condições ambientais, os problemas sanitários e o perfil epidemiológico das doenças e agravos atuando em ações de saneamento básico;

3. Ambiente social: impacto para melhoria nas condições de vida de populações vulneráveis visando à prevenção de doenças, ampliando os sistemas de abastecimento de água e de esgotamento sanitário e controle da qualidade de água para consumo humano proveniente de sistemas de abastecimento público;

4. Ambiente político: a volatilidade do aspecto político impacta diretamente o estabelecimento de prioridades e execução de projetos e metas institucionais. A alta direção orienta a estratégia para o prosseguimento dos projetos que serão implantados.

## 4.2 Contexto Interno

Os valores culturais internos da FUNASA estão relacionados com a ética, equidade, transparência, eficiência, eficácia, efetividade, valorização dos servidores e compromisso socioambiental. O organograma da FUNASA está estruturado de acordo com a Figura 4.1:

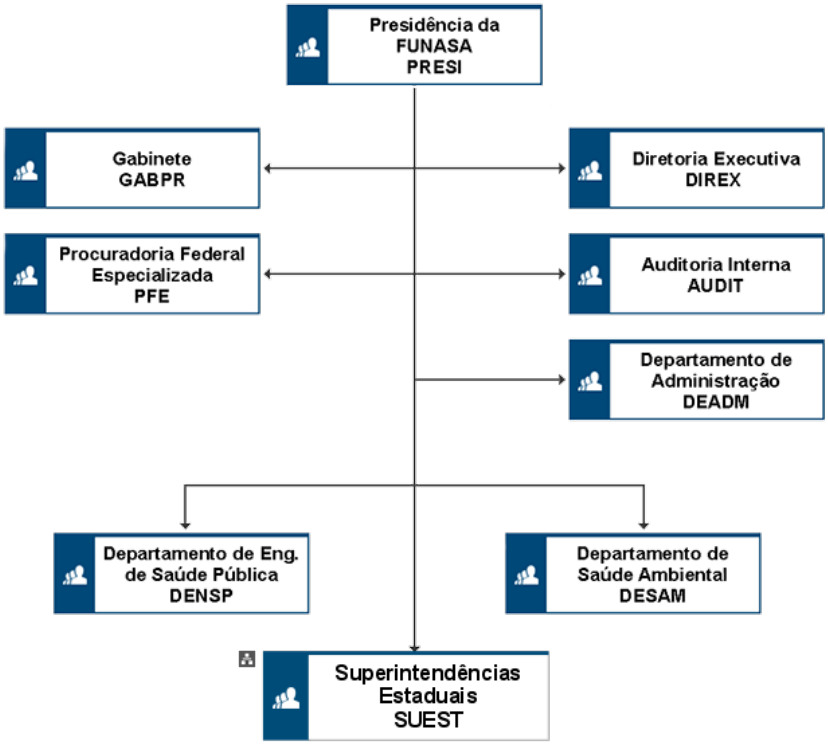


**Figura 4.1:** Organograma Funasa. (Fonte: [44]).

Atualmente a estrutura organizacional da FUNASA possui três departamentos (administração, engenharia de saúde pública e saúde ambiental), uma diretoria executiva, um gabinete, além de uma procuradoria especializada, uma auditoria interna e as superintendências estaduais, todas ligadas ao presidente do órgão. As duas principais áreas que conduzem a missão institucional da FUNASA são os departamentos de engenharia de saúde pública e de saúde ambiental, e as demais áreas são consideradas meios que contribuem para o alcance dos objetivos.

O setor responsável pela área de TI na FUNASA, é subordinado ao departamento de administração e é chamado de Coordenação Geral de Modernização e Tecnologia da Informação (CGMTI), responsável por organizar, manter e fornecer os serviços de recursos de TI, bem como desenvolver, implementar, documentar e manter sistemas de informação, visando atender às necessidades das demais diretorias da FUNASA. A estrutura organizacional da CGMTI conta com duas coordenações, de acordo o que ilustra a Figura 4.2:

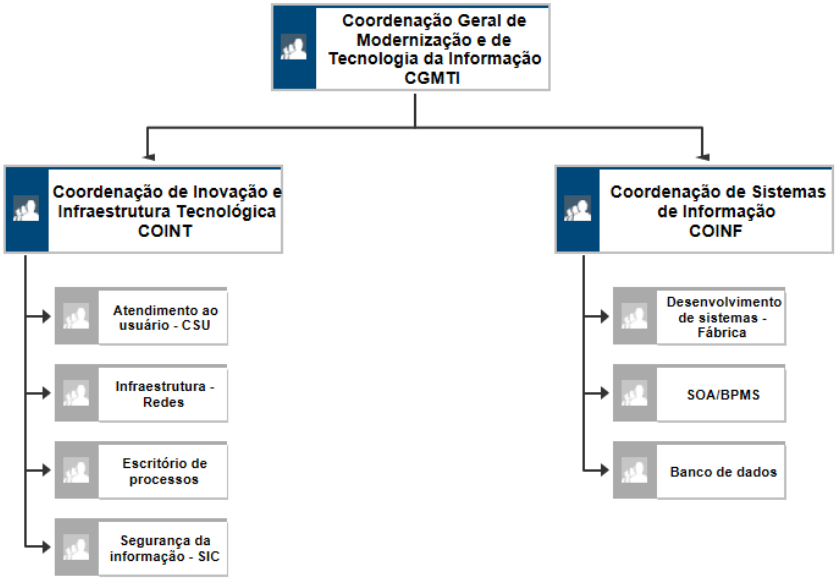


**Figura 4.2:** Organograma da CGMTI. (Fonte: [44]).

A CGMTI conta com a Coordenação de Inovação e Infraestrutura Tecnológica (COINT) e a Coordenação de Sistemas de Informação (COINF), que possuem 4 e 3 áreas respectivamente, e compete a ambas, às contratações relacionadas com tecnologia da informação e comunicações para toda FUNASA, incluindo suas superintendências estaduais, contexto vital para o alcance dos objetivos da FUNASA, pois os recursos de TI utilizados, ajudam às áreas no sucesso de suas metas institucionais [45].

O atual Modelo de Contratação de TI (MCTI) da FUNASA é orientado pela IN-SLTI/MP 04, que é composto por fases que contêm fluxos ou processos, atividades, atores, e se traduzem na forma de artefatos preenchidos para cada uma de suas fases, gerando a ideia de que, se os artefatos são elaborados, a fase está em conformidade com a norma. A Figura 4.3 mostra uma visão geral do Modelo de Contratações de Soluções de TI proposto pela SLTI/MP:

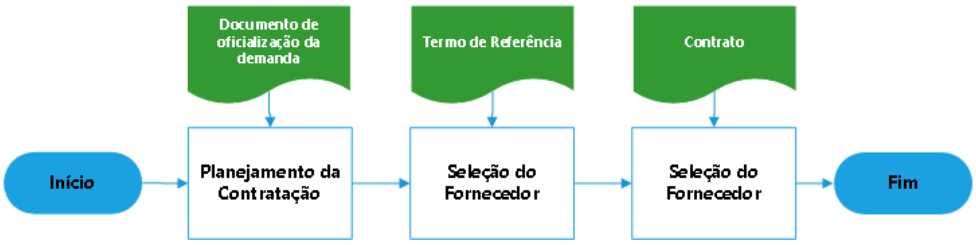


**Figura 4.3:** Modelo de contratação de soluções de TI. (Fonte: Adaptado de [34] ).

No modelo apresentado, a gestão de riscos nas contratações de TI é prevista na etapa de planejamento da contratação e deve ser obtida com o preenchimento e entrega de um artefato chamado "Análise de Riscos". No artefato são identificados os riscos que podem comprometer o sucesso da contratação e da gestão contratual, apresentando as ameaças que possam impedir que a solução, em processo de aquisição, não alcance os resultados que atendam às necessidades da contratante [35].

## 4.3 Contexto da Gestão de Riscos

As contratações de TI na FUNASA, seguem o roteiro estabelecido na IN-SLTI/MP 04, contudo, a gestão de riscos se reduz apenas ao preenchimento do artefato. A identificação dos riscos é feita de maneira abrangente, sem a especificação de critérios objetivos e controles internos. Tal cenário é verificado também pela quantidade de projetos cancelados ou ainda em andamento, nos últimos 3 anos na FUNASA, de acordo o que ilustra a Figura 4.4:

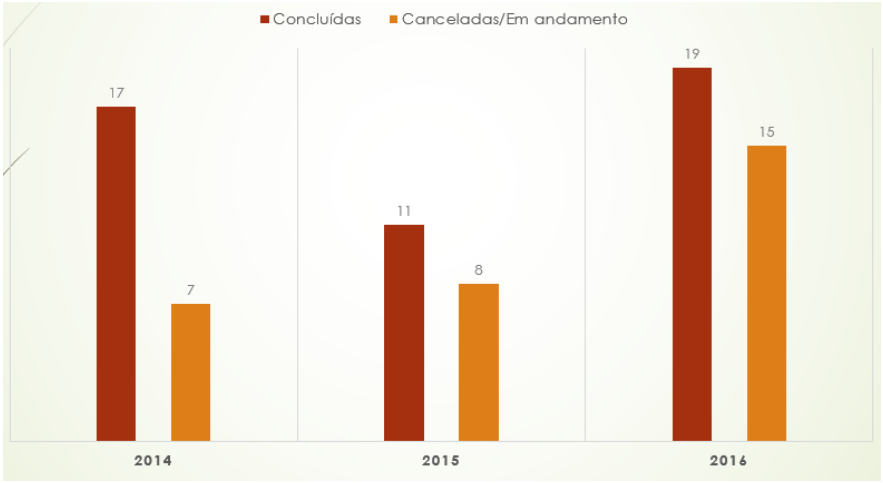


**Figura 4.4:** Quantitativo de aquisições em TI por ano. (Fonte: Elaboração própria.).

Ao analisar os dados, verifica-se que uma grande quantidade de projetos de contratação de TI na FUNASA sofreram com alguma interrupção ou atraso para sua conclusão. Muitas contratações iniciadas em um ano, só apresentaram algum tipo de solução, seja pela conclusão, seja pelo adiamento, em anos posteriores, o que faz com que alguns projetos sejam contabilizados novamente no respectivo ano. A FUNASA possui um direcionamento para gestão de riscos sobre o seu processo de aquisição de TI, mas que se restringe a uma normatização interna retirada do artefato de análise de riscos da norma IN-SLTI/MP 04/2014, conforme ilustra a Figura 4.5 constante no manual de aquisições [32]:

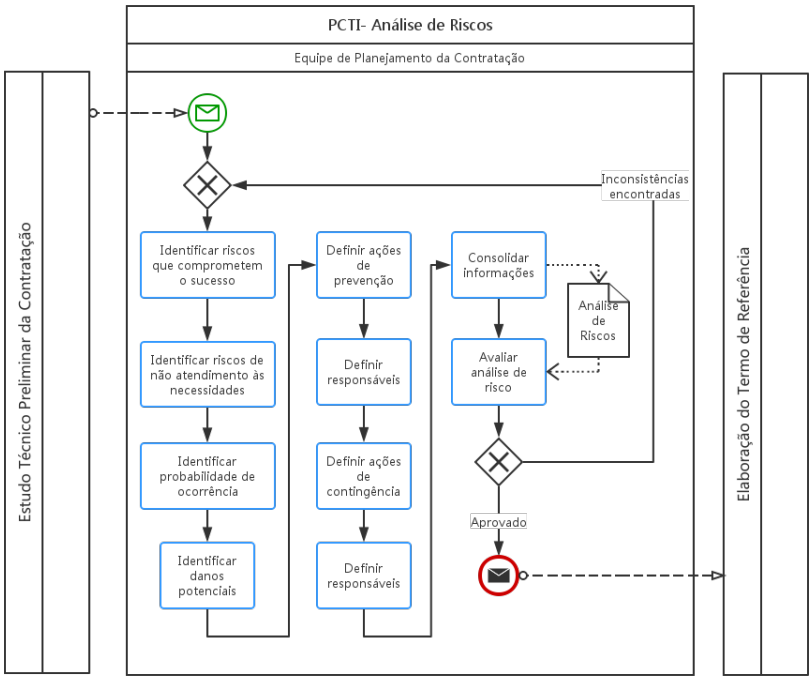


**Figura 4.5:** Processo de Análise de Riscos. (Fonte: Adaptado de [32]).

A normatização interna não representa efetividade em gestão de riscos no processo de contratação de TI no órgão, pelo contrário, se reduz apenas à produção de artefatos decorrentes do processo citado, sem evidências aparentes da implantação de controles, tratamento de riscos e monitoração dos eventos de riscos, entre outras ações desejadas.

## 4.4 Documentos relacionados ao Contexto

O normativo aplicável às contratações de serviços de TI é bastante extenso e o processo de sua catalogação é complexo. Devem-se considerar os aspectos constitucionais, de organização administrativa, orçamentários, de licitações e contratos, de segurança da informação, relativos a políticas governamentais e de requisitos das instâncias do controle, além de se considerar as leis, normas e modelos de governança de TI. Os principais documentos internos relacionados ao contexto da presente pesquisa são:

1. Plano Plurianual da FUNASA (PPA): principal instrumento de planejamento estratégico da FUNASA, previsto no artigo 165 da Constituição Federal, regulamentado pelo Decreto 2.829/98. Estabelece diretrizes, objetivos e metas da FUNASA para um período de 4 anos, organizando as ações do governo em programas que resultem em bens e serviços para a população;

2. Plano Estratégico de TI (PETI): instrumento que visa traçar as ações da área de TI alinhadas aos objetivos estratégicos institucionais, tendo como resultado um documento que estabelece metas a curto e médio prazo para consecução da sua missão. Apresenta objetivos estratégicos relacionados às contratações de TI num período de 3 anos, atualmente 2016 a 2019;

3. Plano Diretor de Tecnologia da Informação (PDTI) 2016/2019: instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TI que visa atender às necessidades tecnológicas e de informação da FUNASA no período de 2016 a 2019. As metas previstas no PDTI constam no planejamento para as aquisições de TI no período de 2016 a 2019;

4. Norma interna MNP-SI-007-2014: metodologia de gestão de riscos de segurança da informação e comunicações para os ativos de TI, processos e usuários da FUNASA [32];

5. Política de Segurança da Informação e Comunicações: prevê que a FUNASA deve identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação.

Entretanto, apesar da contribuição que tais documentos trazem para as contratações de TI na FUNASA, são necessários mais esforços na capacitação dos servidores públicos com foco na adoção de melhores práticas para a gestão de riscos. O presente trabalho propõe alternativas para minimizar a possibilidade da ocorrência de impactos sobre as contratações de TI na FUNASA, o que será proposto no próximo capítulo com a metodologia de gestão de riscos elaborada a partir do diagnóstico da situação atual e da revisão de literatura.

# Capítulo 5

# Proposta de Metodologia para Gestão de Riscos das Contratações de TI

Este capítulo descreve a proposta de solução para o gerenciamento dos riscos nas contratações de TI na FUNASA. Nele é demonstrado todo arcabouço composto de processos, técnicas e artefatos que farão parte da metodologia elaborada.

## 5.1 Elaboração da Metodologia Proposta

O Guia do TCU (2012) descreve que o gestor público é quem deve definir o processo de trabalho de contratação de TI que o órgão seguirá, à luz da legislação e da jurisprudência, podendo ser utilizados diversos instrumentos como padrões e *frameworks* [24]. O processo principal da metodologia de gestão de riscos para as contratações de TI da FUNASA, segue a proposta estabelecida na Figura 5.1, de acordo com o que preconiza o art. 13 da IN-SLTI/MP 04/2014. Assim, o modelo proposto está em conformidade legal e os processos selecionados constam em praticamente todos os modelos estudados, como os de identificação, análise e avaliação e tratamento dos riscos. Além disso, a proposta apresenta um processo de monitoramento e de geração de informações que permite a comunicação e a tomada de decisões sobre as prioridades para a contratação de recursos de TI. A metodologia é baseada na ABNT NBR ISO 31000 (2009) e estabelece atividades de ponta a ponta, visando direcionar a implantação da metodologia de gestão de riscos nas contratações de TI especificamente da Fundação Nacional de Saúde (FUNASA).

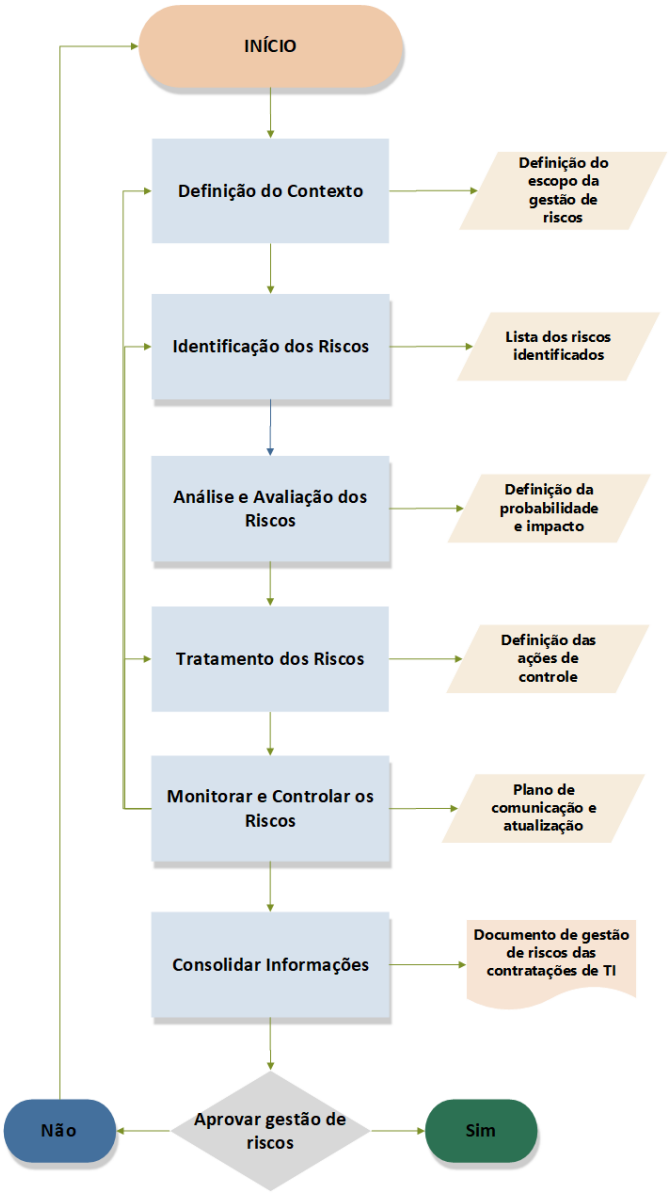


**Figura 5.1:** Processo de gestão de riscos das contratações de TI para a FUNASA. (Fonte: Adaptado de [54]).

A gestão dos riscos das contratações de TI permeia todas as fases do processo de planejamento da contratação das soluções de TI e deve ser um processo iterativo, porque novos riscos podem surgir durante a evolução do projeto. Na FUNASA, os riscos identificados em uma semana podem não ser idênticos aos riscos identificados para o mesmo negócio na próxima semana [16]. Assim, a metodologia proposta apresenta mecanismos de acompanhamento e revisão dos riscos identificados, que proporcionam maior controle das ameaças que surgem durante o processo de contratação, contribuindo para o devido sucesso da contratação dos bens ou serviços de TI. Ao final, os riscos levantados devem ser consolidados em um artefato final chamado "Análise de Riscos", de acordo com o

estabelecido na norma IN-SLTI/MP 04/2014 [35]. A expressão "Gestão de Riscos" do modelo proposto está relacionada ao processo de "Análise de Riscos" da referida norma. A metodologia proposta obedece aos princípios estabelecidos na norma ABNT NBR ISO 31000 (2009) na qual a gestão de riscos [54]:

- Cria valor: contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho do processo de contratação de TI da FUNASA;
- É parte integrante dos processos organizacionais: não é uma atividade autônoma separada do processo de contratação de TI;
- É parte da tomada de decisões: auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação para as contratações de TI;
- Aborda explicitamente a incerteza: leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada;
- É sistemática, estruturada e oportuna: contribui para a eficiência e para os resultados consistentes nas contratações de TI, comparáveis a outros projetos e confiáveis;
- É baseada nas melhores informações disponíveis: tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas;
- É feita sob medida: está alinhada com o contexto interno e externo da FUNASA e com o perfil do risco;
- Considera fatores humanos e culturais: reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização;
- É transparente e inclusiva: o envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada;
- É dinâmica, interativa e capaz de reagir a mudanças: continuamente percebe e reage às mudanças. Na medida em que acontecem eventos externos e internos, o contexto e o conhecimento modificam-se, o monitoramento e a análise crítica de riscos são realizados, novos riscos surgem, alguns se modificam e outros desaparecem; e
- Facilita a melhoria contínua da organização: desenvolve e implementa estratégias para melhorar a sua maturidade na gestão de riscos nas contratações de TI da FUNASA.

A proposta de metodologia de gestão de riscos das contratações de TI da FUNASA possui um total de 20 tarefas agrupadas em 11 atividades organizadas em 6 processos. O Quadro 5.1 apresenta um resumo da metodologia proposta com sua quantidade de processos, tarefas e atividades:

**Quadro 5.1:** Estrutura do processo de gestão de riscos das contratações de TI. (Fonte: Adaptado de [36]).

| **Processo** | **Atividades** | **Tarefas** |
|---|---|---|
| Definição do Contexto | 1 | 3 |
| Identificação dos Riscos | 2 | 6 |
| Análise e Avaliação dos Riscos | 3 | 5 |
| Tratamento dos Riscos | 2 | 3 |
| Monitorar e Controlar os Riscos | 2 | 2 |
| Consolidar Informações | 1 | 1 |

As atividades e tarefas foram elaboradas a partir dos modelos estudados e das metodologias já adotadas pela APF. Diante da realidade identificada na FUNASA, foram adaptadas tarefas estabelecidas pelo o PMBOK (2013), *The Institute of Risk Management* - IRM (2002), *The Orange Book* (2004), ISO 31000 (2009), Metodologia de Gestão de Riscos de Segurança da Informação do Ministério do Planejamento (2016), Guia de Orientação para o Gerenciamento de Riscos (2013) e de autores como Chapman e Ward (2003). Além disso, toda metodologia apresenta conformidade com as leis e normas relacionadas às contratações de TI, como a IN-SLTI/MP 04/2014.

Devido à complexidade do assunto, a grande rotatividade dos envolvidos e a característica multidisciplinar (envolvimento de áreas diversas como a área requisitante e a área administrativa) da gestão de risco no processo de contratação de TI da FUNASA, buscou-se a apresentação de uma metodologia com profunda documentação e com o devido detalhamento das ações, de maneira que, auxilie no nivelamento das informações, mesmo daqueles que nunca tiveram contato com a matéria de gestão de riscos nas contratações de TI. Os processos da metodologia são descritos por meio de atividades e tarefas, informando os responsáveis, as entradas, as saídas e as técnicas necessárias para a execução das mesmas. A imagem 5.2 demonstra o quadro geral com os processos, atividades e tarefas da metodologia proposta:

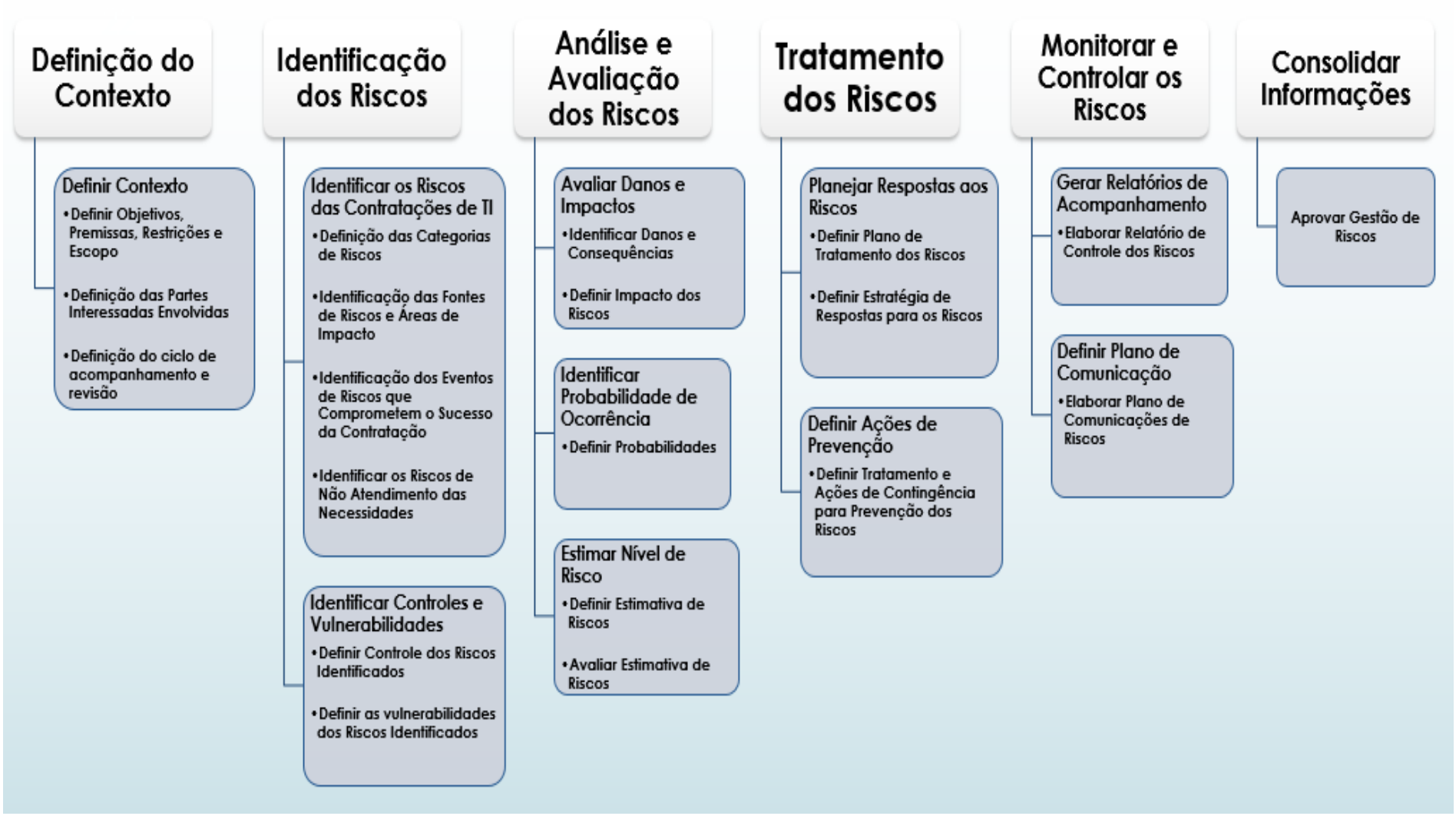


**Figura 5.2:** Quadro geral da metodologia da gestão de riscos das contratações de TI. (Fonte: Adaptado de [36]).

Além disso, para a FUNASA, tornou-se necessária a demonstração dos resultados das tarefas em *templates*, com exemplos associados a cada tarefa apresentada, para tornar a implementação da metodologia menos complexa, mais ágil, de fácil entendimento, com maior qualidade e com melhores resultados práticos.

### 5.1.1 Papéis organizacionais

Os papéis definem as formas de comportamento associadas as tarefas e diferenciam as funções e os cargos exercidos pelos indivíduos nas responsabilidades dos processos, atividades e tarefas [76]. Na metodologia proposta, os papéis organizacionais são:

**Autoridade Competente:** responsável por prover os recursos necessários à gestão de riscos das contratações de TI (no caso da FUNASA, o diretor de Administração); Institui a equipe responsável pelas atividades de gestão de riscos; aprova pontos importantes relativos à gestão de riscos tais como: artefatos, restrições e aprimoramento da metodologia de gestão de riscos para as contratações de TI;

**Equipe de planejamento da contratação:** de acordo com o art. 2º da IN-SLTI/MP 04/2014, fazem parte da equipe de contratação os integrantes das áreas de TI, administrativa e da área requisitante da solução de TI, são eles os responsáveis por executar as atividades de gestão de riscos e coordenar esforços para identificar e estimar riscos, propor melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados. São nomeados no início do planejamento da contratação de TI, assinam e aprovam a gestão de riscos elaborada;

**Gestor de TI:** responsável pela área de TI da organização na qual a metodologia será implementada, ele proverá informações para a gestão de riscos. Tem o papel de coordenar o fornecimento de informações necessárias à identificação e à estimativa de riscos e realizar melhorias necessárias quando as análises indicarem.

## 5.2 Definição do Contexto

A atividade de identificação do contexto de riscos deve definir o ambiente no qual a gestão dos riscos da contratação de TI está inserida, analisando qual o escopo de atuação, as premissas, restrições e os responsáveis pela atividade. Os objetivos dão subsídios para a elaboração da gestão de riscos, informando qual o resultado esperado para a metodologia. O escopo define onde atuará a gestão de riscos, explicitando qual natureza da contratação, quais unidades envolvidas (divisões, setores, departamentos, processos, sistemas) e quais unidades que não serão tratadas [54]. Essa análise deve focar na natureza das atividades

e das informações em cada unidade e as justificativas para a escolha das unidades devem ser documentadas. As tarefas previstas para o processo estão definidas no Quadro 5.2:

**Quadro 5.2:** Estrutura do processo de definição do contexto. (Fonte: Adaptado de [54, 36, 16]).

| **Definição do contexto** | | |
|---|---|---|
| **Atividades** | **Tarefas** | **Fonte** |
| Definição do contexto | Definir Objetivos, Premissas, Restrições e Escopo | [54] |
| | Definição das Partes Interessadas Envolvidas | [36] |
| | Definição do Ciclo de Acompanhamento e Revisão | [16] |

As tarefas indicam para uma definição introdutória das informações do projeto de contratação de TI, podem ser levados em consideração as leis e demais documentos internos que sejam necessários para a definição do contexto da gestão de riscos. Todas as informações devem ser registradas e atualizadas para o devido acompanhamento do projeto. A definição do contexto pode ainda considerar o estabelecimento de parâmetros externos e internos que se relacionam com o ambiente de gestão de riscos do projeto de contratação de TI em questão [54]. As entradas, técnicas utilizadas, requisitos do processo e saída esperada são descritas na Figura 5.3:

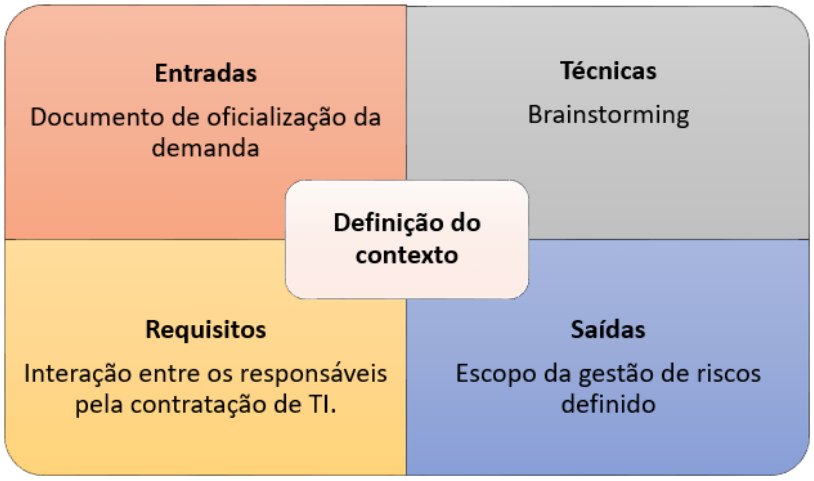


**Figura 5.3:** Definição do contexto dos riscos: entradas, técnicas, requisitos e saídas. (Fonte: Elaboração própria).

A entrada do processo de definição do contexto, considera o primeiro documento a ser produzido no planejamento da contratação de TI, que é o documento de oficialização da demanda, na qual definem-se o objetivo, escopo e a equipe integrante que irá conduzir o planejamento da contratação da solução de TI. Para a definição do escopo da gestão de riscos é necessário que a equipe de planejamento se reúna e interaja entre si colhendo as informações iniciais dispostas no documento de oficialização da demanda e documentando de acordo como solicitado nas tarefas.

### Definir Objetivos, Premissas, Restrições e Escopo

A equipe de planejamento da contratação deve iniciar o projeto de gestão de riscos da contratação de TI informando os objetivos genéricos e os objetivos específicos da contratação (tais como os relacionados aos processos de negócios ou nas informações de sistemas, obrigações legais ou regulatórias, atividades que podem afetar a ordem pública que requerem alta disponibilidade, sistemas e informações cruciais para a tomada de decisões). Além disso, devem ser identificados os tipos de restrições que se apliquem (tais como técnicas, jurídicas, financeiras, de prazos) e descrever em detalhes as premissas, informando, se necessário, valores como de prazo ou de orçamento. A equipe de planejamento da contratação responsável pela gestão de riscos deve identificar também as unidades relacionadas ao escopo do projeto que mereçam atenção e que devam ser tratadas na gestão de riscos [36].

A condição necessária para finalização da tarefa é a definição dos objetivos, premissas e restrições do projeto de contratação de TI e devem ser documentados de acordo com a Figura 5.4:

| OBJETIVOS, ESCOPO, PREMISSAS E RESTRIÇÕES DO PROJETO | |
|---|---|
| **Objetivos do Projeto:** | Descrição dos Objetivos |
| **Nível de criticidade:** | (Baixa, Média, Alta) |
| **Escopo do Projeto:** | Descrição do Escopo |
| **Premissas do Projeto:** | Descrição das Premissas |
| **Restrições do Projeto:** | Descrição das Restrições |

**Figura 5.4:** Template para o registro de objetivos, escopo, premissas e restrições do projeto. (Fonte: Elaboração própria).

As atividades dos integrantes da equipe de planejamento da contratação não devem ser realizadas de forma isolada. Para o gerenciamento dos riscos das contratações de TI, é necessário que haja, entre a equipe de planejamento, interação durante todo o ciclo do projeto. Nesta primeira tarefa, a equipe de planejamento da contratação deve se encontrar em reuniões iniciais com o objetivo de obter ideias em uma sessão tradicional de *brainstoming* de forma livre, de modo que os participantes interajam entre si e coletem informações que possam dar subsídios para as respostas sobre os objetivos, premissas, restrições e escopo do projeto, preenchendo inicialmente o documento de identificação dos riscos com os dados coletados [67]. A equipe de planejamento da contratação deverá coletar as seguintes informações:

- Objetivos da contratação da solução de TI;

- Nível de criticidade do projeto;
- Regulamentações específicas;
- Restrições financeiras;
- Restrições de prazo;
- Restrições técnicas.

### Definição das Partes Interessadas Envolvidas

Para a tarefa de definição das partes interessadas envolvidas, devem ser identificados os responsáveis por cada unidade levantada no escopo, informando os dados de contato e as situações as quais as partes interessadas deverão ser comunicadas. Poderá ser utilizada a técnica de reuniões do tipo *brainstorming* para obtenção das informações, com interação livre dos participantes.

A condição para finalização da tarefa é que os profissionais estejam identificados e papéis atribuídos. A tarefa pode ser documentada de acordo com a Figura 5.5:

| DEFINIÇÃO DAS PARTES INTERESSADAS ENVOLVIDAS | | | | | |
|---|---|---|---|---|---|
| Nome | Unidade | Telefone | Email | Papel | Responsabilidade |
| Nome1 | Unidade1 | Telefone1 | Email1 | Chefe | Responsabilidade |

**Figura 5.5:** Template para o registro das partes interessadas. (Fonte: Elaboração própria).

As informações necessárias desta tarefa, são responsabilidade da equipe de planejamento que deverá levantar os seguintes dados:

- Informações sobre profissionais da organização e organograma;
- Informações sobre as unidades relacionadas com a contratação de TI.

### Definição do Ciclo de Acompanhamento e Revisão

O registro dos riscos é uma tarefa iterativa que deve ser desenvolvida durante todo o ciclo de vida do projeto [16]. Dessa maneira, devem ser definidos, no início do processo de gestão de riscos, um cronograma de acompanhamento e revisão dos riscos identificados, atualizando os documentos com as informações necessárias.

A responsabilidade da tarefa ficará à cargo da equipe de planejamento da contratação que deverá elaborar o cronograma com o ciclo de acompanhamento e revisão de acordo com a Figura 5.6:

| DEFINIÇÃO DO CICLO DE ACOMPANHAMENTO E REVISÃO | | |
|---|---|---|
| Data | Ação | Descrição |
| 10/10/2017 | Acompanhar | Validar informações sobre o primeiro ciclo de identificação dos riscos. |

**Figura 5.6:** Template para a definição do ciclo de acompanhamento. (Fonte: Elaboração própria).

A equipe poderá utilizar a reunião inicial das tarefas anteriores, com a utilização da técnica de reuniões do tipo *brainstorming* para obtenção das informações, para reunir todas as informações necessárias para a tarefa de definição do ciclo de acompanhamento e revisão. No final da tarefa, a equipe deverá ter documentado as informações sobre um cronograma com marcos de acompanhamento e revisão da identificação dos riscos do projeto.

## 5.3 Identificação dos Riscos

A identificação dos riscos é o segundo processo da metodologia de gestão de riscos das contratações de TI da FUNASA. Nele os eventos que podem afetar o projeto, reduzindo ou eliminando a probabilidade da organização de atingir seus objetivos, são levantados, juntamente com sua descrição, suas características e consequências [16]. Nesse primeiro instante, verifica-se o que pode dar errado no processo de aquisição durante todo o ciclo de vida do projeto, procurando identificar potenciais consequências e vulnerabilidades existentes, avaliando a extensão de tais ameaças [59]. Esta etapa deve gerar uma lista abrangente de riscos, baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos das contratações de TI [54]. Trata-se da identificação dos riscos com uma priorização, focando nos eventos possíveis e suas vulnerabilidades descobertas. Importante destacar que existem ameaças e vulnerabilidades que impactam a organização como um todo e, dessa forma, deve-se priorizar o tratamento dessas ameaças [36]. O Quadro 5.3 destaca a estrutura de atividades e tarefas previstas para o processo de identificação de riscos na metodologia proposta:

**Quadro 5.3:** Estrutura do processo de identificação dos riscos. (Fonte: Adaptado de [34, 67, 35, 36]).

| **Identificação dos Riscos** | | |
|---|---|---|
| **Atividades** | **Tarefas** | **Fonte** |
| Identificar os Riscos das Contratações de TI | Definição das Categorias de Riscos | [34] |
| | Identificação das Fontes de Riscos e Áreas de impacto | [67] |
| | Identificação dos Eventos de Riscos que Comprometem o Sucesso da Contratação | [35] |
| | Identificar os Riscos de Não Atendimento das Necessidades | [35] |
| Identificar Controles e Vulnerabilidades | Definir Controle dos Riscos Identificados | [36] |
| | Definir as Vulnerabilidades dos Riscos Identificados | [36] |

De acordo com a IN-SLTI/MP 04/2014, a equipe de contratação será responsável pelo processo de identificação dos riscos. As tarefas do processo de identificação dos riscos podem ser realizadas em reuniões, com o uso de listas de verificação como a do Apêndice A, que apresenta uma lista com fontes de riscos já conhecidas, e além disso, o Apêndice C, que apresenta uma lista com riscos e controles já identificados em outros projetos relativos ao processo de planejamento de contratações de TI, o que contribui para tornar o processo de identificação dos riscos mais produtivo. Caso seja necessário, a equipe de planejamento poderá consultar outras áreas envolvidas para resolução de dúvidas e coleta de informações necessárias para a identificação dos riscos. As entradas, técnicas utilizadas, requisitos do processo e saída esperada são descritas na Figura 5.7:

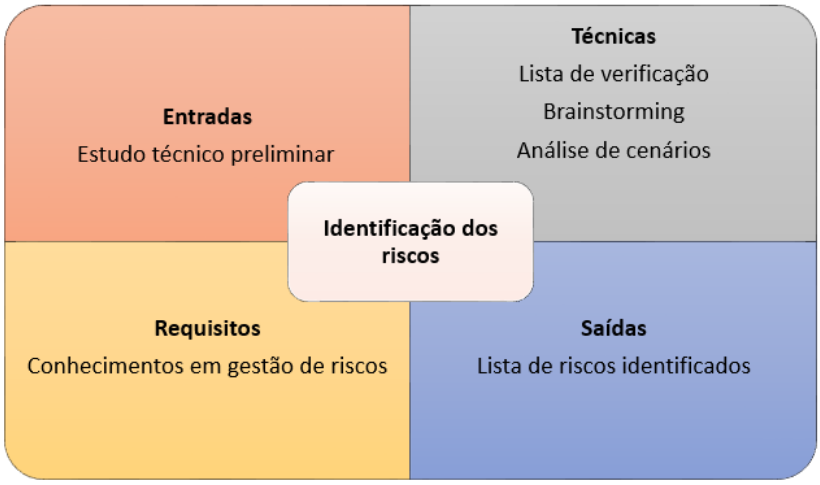


**Figura 5.7:** Processo de identificação dos riscos: entradas, técnicas, requisitos e saídas. (Elaboração própria).

A entrada considera o documento de estudo técnico preliminar da contratação, no qual são definidos as necessidades de negócio e as especificações técnicas relativas à esco-

lha da solução de TI. O documento contribui para que a equipe de planejamento possa desenvolver as atividades necessárias à identificação de riscos do projeto. Entretanto, a etapa de identificação pode acontecer paralelamente ao estudo técnico preliminar, já que se trata de um processo iterativo e incremental, desde que toda atualização do documento do estudo técnico seja refletida também no processo de gestão dos riscos.

Chapman (2011) apresenta que entre as técnicas mais úteis para identificação de riscos, as reuniões com debate sobre os riscos, são consideradas as de melhor resultado, assim, a utilização da técnica de *brainstorming*, que se caracteriza por estimular a produção livre de grandes quantidades de ideias em um curto espaço de tempo (como em reuniões), se configura como mais adequada em conjunto com as técnicas de listas de verificação (*checklists*) e análise de cenários, que são consideradas de baixa complexidade e contribuem para sistematizar a identificação os riscos que afetem a entrega de valor, para uma melhor avaliação dos riscos levantados [16]. Thamhain (2013) complementa que projetos que envolvam pessoas sem um contato anterior com o tema de gestão de riscos, uma abordagem de *brainstorming* é inicialmente recomendada, juntamente com as listas de verificação, reservadas para estimular a produção de informação. As listas de verificação são rápidas de usar e fornecem guias úteis para a equipe envolvida com boa profundidade de experiência, especialmente para projetos similares ou de mesma natureza [78].

### 5.3.1 Identificar os Riscos das Contratações de TI

Nesta atividade, a equipe de planejamento da contratação deverá identificar os principais riscos que possam comprometer o sucesso do processo de contratação. Para estar em conformidade com a norma IN-SLTI/MP 04/2014, a metodologia apresentará as duas atividades de identificação que constam na norma: "Identificação dos Riscos que Comprometem o Sucesso da Contratação" e "Identificar Riscos de Não Atendimento das Necessidades". As duas atividades apresentam similaridades em sua execução e a principal diferença está no tipo de risco relacionado a cada etapa. Para a primeira, o foco está nos riscos relacionados ao processo de contratação e, para a segunda, o objetivo é identificar riscos relacionados à solução contratada. Dessa maneira, a mesma estrutura de elaboração e execução das atividades e tarefas serão contempladas para os dois subprocessos de identificação dos riscos da norma.

De acordo com a NBR ISO 31000 (2009), o processo de identificação dos riscos parte do pressuposto da identificação das categorias dos riscos, fontes de riscos, áreas de impacto e os eventos de riscos que comprometem o sucesso da contratação. As fontes de riscos podem ser consideradas: pessoas sem capacitação, desmotivadas, processos sem segregação de funções, sistemas obsoletos, sem manual, estruturas em que há falta de clareza das funções, infraestrutura instalações/leiaute inadequados, tecnologia, externos

à instituição. Para a identificação das áreas de impacto, devem ser mapeadas as unidades organizacionais que serão influenciadas com os eventos de riscos. Por fim, a tarefa de identificação dos eventos demonstra os riscos, registrando em documento os atributos: número identificador, categoria de risco, data de identificação, descrição do risco e proprietário do risco [54].

### Definição das Categorias de Riscos

A categorização subsidia as etapas posteriores da identificação dos riscos e auxilia na organização dos riscos levantados. Os riscos serão classificados em internos e externos. Os riscos internos poderão ser categorizados do tipo [34]:

1. Financeiros: incerteza em relação às fontes de financiamento e orçamento;
2. Humanos: relacionados à disponibilidade, contratação ou capacitação das equipes;
3. Processos: relacionados à falta de definição de processos críticos específicos assim como de papéis e responsabilidades, autoridade para aprovação;
4. Sistemas: relacionados à adequação de sistemas de informação;
5. Técnico: relacionados aos requisitos técnicos que compõem a contratação de TI;
6. Parceiros/Fornecedores: forma contratual e definição de papéis e responsabilidades, capacitação de fornecedores, processo de seleção;
7. Outros: outros riscos específicos, internos da organização que não se enquadram nas categorias acima.

Os riscos externos poderão ser categorizados como [34]:

1. Políticos: mudança de governo; mudança no cenário político; decisões sobre políticas interministeriais; mudanças na máquina do governo; terrorismo etc.;
2. Econômico: inflação; variação cambial afetando custos nas transações internacionais; taxa de juros; efeitos da economia global na economia brasileira; ações da concorrência internacional, etc.;
3. Socioculturais: mudanças demográficas afetando a demanda por serviços; mobilidade de classes sociais; mudança de expectativa dos cidadãos e da sociedade devido à globalização; conflitos sociais etc;
4. Tecnológicos: tecnologias emergentes; Internet; obsolescência dos sistemas atuais; mudança na competitividade estrutural com base no uso de novas tecnologias; oportunidades advindas de avanços tecnológicos;

5. Legal/Regulatório: novas leis ou mudanças de marcos regulatórios em termos de qualidade, segurança, meio ambiente, saúde, trabalhista; etc;
6. Ambiental: desastres naturais, ecológicos, climáticos (enchentes, deslizamentos, secas).

As categorias dos riscos devem ser documentadas, de acordo com o template na Figura 5.8:

| DEFINIÇÃO DAS CATEGORIAS DE RISCOS | | |
|---|---|---|
| Classificação | Categoria | Descrição |
| Interno | Financeiros | Incerteza em relação às fontes de financiamento e orçamento. |
| Externo | Políticos | Mudança de governo; mudança no cenário político; decisões sobre políticas interministeriais; mudanças na máquina do governo; terrorismo etc.; |

**Figura 5.8:** Template para o registro das categorias de riscos. (Fonte: Elaboração própria).

Outras categorias de riscos podem ser acrescentadas, caso seja necessário, de acordo com a realidade e adesão da metodologia dentro do órgão. As categorias auxiliam os gestores a observarem os tipos de riscos que podem apresentar maior incidência, maiores custos para tratamento ou riscos com maior impacto sobre as contratações de TI da FUNASA.

### Identificação das Fontes de Riscos e Áreas de Impacto

A análise de riscos envolve a apreciação das fontes de risco [54]. Para Thamhain (2013) todas as fontes de dados disponíveis devem ser usadas na avaliação dos riscos [78]. A identificação das fontes deve fazer com que a equipe de planejamento da contratação informe todo tipo de ativo na qual um risco pode surgir (áreas de negócio, processos, escopo, tempo, custo, recursos, fornecedores, qualidade, legalidade, pessoas, tecnologia) e qual área de impacto relacionada (área requisitante da solução, área técnica, área administrativa entre outras) [67]. A equipe de planejamento pode considerar informações contidas em projetos similares, melhores práticas, literatura, manuais técnicos, experiência e julgamento técnico para tornar a identificação das fontes de riscos mais completa [78]. A identificação das fontes de risco contribui para elaboração de estruturas analíticas dos riscos (EAR) como modo de listar de forma hierárquica os riscos, de acordo com a Figura 5.9 [67]:

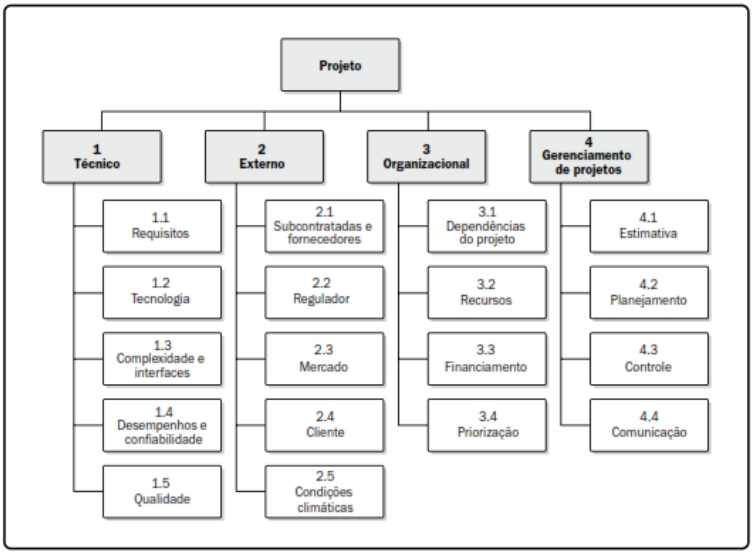


**Figura 5.9:** Exemplo de uma estrutura analítica dos riscos (EAR). (Fonte: Elaboração própria) .

A estrutura analítica dos riscos da contratação de TI em questão contribui para que a equipe de planejamento verifique onde há uma maior probabilidade de ocorrência de eventos negativos, por exemplo, na área de negócio, tempo, pessoas, entre outros, auxiliando a proposição de melhorias para a respectiva fonte.

A equipe de planejamento da contratação e os responsáveis pelas unidades da organização podem auxiliar a identificação das fontes de riscos, informando possíveis focos de problemas para a contratação de TI pretendida. Ao final da tarefa, as fontes de riscos e áreas de impacto devem ser documentadas como proposto na Figura 5.10:

| FONTES DE RISCOS E ÁREAS DE IMPACTO | | | | | |
|---|---|---|---|---|---|
| ID | Fonte | Unidade | Responsável | Descrição da função | Data |
| 01 | Pessoas | Financeiro | Maria | Chefe da área financeira, responsável pela utilização da solução de TI a ser contratada. | 09/09/17 |
| 02 | Processos | Administrativo | José | Falta de processo estabelecido para verificação de reajustes financeiros da solução contratada. | 15/09/17 |

**Figura 5.10:** Template para as fontes de riscos e áreas de impacto. (Fonte: Elaboração própria).

Para o levantamento das fontes de riscos e áreas de impacto, a equipe de planejamento poderá utilizar listas de verificação, como a disponível no Apêndice A, com base nas informações históricas e no conhecimento já acumulado pela organização, a partir de contratações anteriores semelhantes e outras fontes de informações. A equipe poderá solicitar informações a outros setores da organização, comunicando diretamente aos responsáveis pelas unidades ou solicitando ao gestor de TI que o faça [67]. As informações necessárias para tarefa de identificação das fontes de riscos e áreas de impacto são:

- Fonte de riscos identificadas e documentadas;
- Unidades organizacionais que podem ser impactadas com relação às fontes de riscos identificadas.

**Identificação dos Eventos de Riscos que Comprometem o Sucesso da Contratação**

O resultado da tarefa deve ser a lista com o registro dos riscos no documento onde são inseridos os eventos que podem causar danos e impactos às contratações de TI. Além disso, os riscos registrados devem ser categorizados, com o resultado coletado pela tarefa "Definição das categorias de riscos" e relacionados às fontes e áreas de impacto contidas na tarefa "Identificação das fontes de riscos e áreas de impacto".

Os riscos identificados devem ser descritos com o maior número de detalhes possível. Um risco pode conter várias ameaças relacionadas com impactos distintos que devem ser mapeados. Considerando a complexidade e a necessidade de projeções futuras, poderá ser utilizada a técnica de lista de verificação ou *checklist* elaborada em projetos de contratação anteriores, em conjunto com a técnica de análise de cenário que fornecerão uma lista de incertezas típicas considerando as perdas que já ocorreram a fim de entender as causas contributivas. A lista de verificação deve ajudar a cobrir adequadamente o escopo e gerar um banco de conhecimentos a partir das experiências em outras contratações.

Um cenário de risco é a descrição de um possível evento que, quando ocorrido, terá um impacto incerto sobre o alcance da contratação de TI. Pode-se usar a seguinte estrutura para a descrição dos eventos de riscos: *"o evento X pode ocorrer, causando o impacto Y, ou então, se uma causa X existe, o evento pode ocorrer, levando ao feito Z"*. Os cenários futuros devem ser identificados presumindo que cada um desses possa ocorrer, desenvolvendo modelos descritivos e considerando suas consequências. A partir de pesquisas internas com as principais tendências, é necessário identificar as mudanças organizacionais que possam ocorrer, mudanças externas, decisões a serem tomadas que possam ter uma variedade de resultados, mudança de escopo, mudanças regulatórias, entre outras. [53]. A

compilação dos resultados pode gerar uma lista de riscos considerando o pior caso, como por exemplo:

- Risco: atraso no processo de contratação. Causa: falta de pessoal especializado. Impacto: Paralisação de serviços essenciais;
- Risco: alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades. Impacto: Atraso na entrega da solução.

A equipe de planejamento da contratação deve documentar os riscos identificados de acordo com o template da Figura 5.11:

| RISCOS QUE COMPROMETEM O SUCESSO DA CONTRATAÇÃO | | | | | | |
|---|---|---|---|---|---|---|
| ID | Categoria | Fonte | Descrição do Risco | Impacto | Responsável | Data |
| 01 | Processos | 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Diretor executivo. | 09/09/17 |
| 02 | Políticos | 01 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Diretor administrativo. | 15/09/17 |

**Figura 5.11:** Template para o registro dos riscos que comprometem o sucesso da contratação. (Fonte:Elaboração própria).

Os riscos identificados devem ser registrados em documento específico da atividade de identificação dos riscos. O documento deve conter os seguintes atributos:

- Número de identificação atribuído ao risco;
- Categoria de risco - identificados na tarefa "Definição das categorias de riscos";
- Fonte do Risco - relacionado à tarefa "Identificação das fontes de riscos e áreas de impacto";
- Descrição do Risco (Evento, causa, dano);
- Impacto;
- Responsável do Risco; e
- Data da identificação;

#### Identificar Riscos de Não Atendimento das Necessidades

Nesta atividade, seguindo a proposta estabelecida no art. 13 da IN-SLTI/MP 04/2014 inciso II, a equipe de planejamento da contratação deverá identificar os principais riscos que possam fazer com que os serviços prestados ou bens fornecidos não atendam às necessidades do órgão contratante, o que poderá resultar na necessidade da realização de uma nova contratação. De forma similar à tarefa anterior de "Identificação dos Riscos que Comprometem o Sucesso da Contratação", a tarefa de identificação dos riscos de não atendimento das necessidades complementa o processo de identificação dos riscos contemplando a identificação de riscos específicos que impactarão as necessidades do projeto.

Como requisito necessário para esta atividade, a equipe de planejamento da contratação deve primeiro ter concluído a tarefa "Identificação das Fontes de Riscos e Áreas de Impacto", caso ainda não tenha identificado as fontes de riscos e áreas de impacto.

Os atributos e técnicas seguirão os mesmos procedimentos estabelecidos na tarefa anterior, com o foco direcionado à identificação de riscos do não atendimento das necessidades após a conclusão do processo de contratação do produto ou serviço de TI. O template descrito na Figura 5.12 refere-se ao registro dos riscos de não atendimento das necessidades:

| RISCOS DE NÃO ATENDIMENTO DAS NECESSIDADES | | | | | | |
|---|---|---|---|---|---|---|
| ID | Categoria | Fonte | Descrição do Risco | Impacto | Responsável | Data |
| 01 | Tecnológico | 01 | Falta de requisito técnico de atendimento das necessidades. | Prestação parcial dos serviços. | Gestor de TI. | 09/09/17 |
| 02 | Financeiro | 01 | Falta de limite orçamentário. | Falta de produtos ou serviços. | Diretor administrativo. | 15/09/17 |

**Figura 5.12:** Template para identificação dos riscos de não atendimento das necessidades. (Fonte: Elaboração própria).

O registro dos riscos se dá no documento de identificação dos riscos, inserindo os danos e o impacto relacionado aos riscos. Como na tarefa de "Identificação dos eventos de riscos que comprometem o sucesso da contratação", os riscos registrados devem ser categorizados, de acordo com o resultado coletado pela tarefa de "Definição das Categorias de Riscos".

### 5.3.2 Identificar Controles e Vulnerabilidades

Os controles são considerados uma reserva de contingência para os riscos conhecidos que não podem ser gerenciados de forma proativa [67]. Ao se identificar os riscos no processo

de contratação de bens e serviços de TI, deve-se estabelecer controles para protegê-los contra as ameaças identificadas. Controles protegem a fonte de risco e evitam que os riscos explorem suas vulnerabilidades e causem danos a ele e ao seu contexto.

Cada fonte de risco pode estar sujeita a uma ou mais ameaças, e neles podem ser aplicados um ou mais controles. Pode ser utilizada lista de verificação, elaborada pela organização, na identificação de possíveis controles associados às ameaças. No processo de identificação dos riscos, os controles são apenas identificados e documentados, nas fases seguintes da proposta, os controles serão classificados, analisados e transformados em ações que darão efetividade aos controles identificados.

As vulnerabilidades podem ser consideradas ameaças associadas aos controles, explorando as fraquezas não implementadas [36]. As vulnerabilidades podem ser exploradas por ameaças e causar danos aos ativos ou à organização. Pode ser elaborado um catálogo de vulnerabilidades relacionadas aos riscos e controles já identificados em projetos anteriores. Dessa maneira, as tarefas desta atividade são:

- Definir controle dos riscos identificados;
- Definir as vulnerabilidades dos riscos identificados associadas aos controles.

### Definir Controle dos Riscos Identificados

Os controles são as formas de se gerenciar o risco, e podem incluir políticas, procedimentos, diretrizes, práticas, estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controles de modo geral tem o efeito de reduzir os riscos por meio de dois fatores [36]:

- Realizam uma redução da exposição de um ativo ao risco, protegendo-o e diminuindo assim a probabilidade de que incidentes ocorram;
- Realiza uma ação da gravidade da consequência em termos abrangência, de duração e de impacto na organização.

Os controles podem ser cadastrados em um catálogo ou banco de informação, considerando informações históricas e no conhecimento acumulado em projetos anteriores, de forma que se forme uma lista de verificação para que a equipe de planejamento elabore os controles dos riscos identificados em reuniões de *brainstorming*. Os controles são concebidos e desenvolvidos com base nos riscos identificados e deve desenvolver ações diretamente ligadas à cada ameaça documentada, informando sua situação (implementado ou não implementado) e justificativa. A equipe de planejamento da contratação deve reunir as informações dos controles dos riscos, identificando e documentando todas as informações.

**Definir as Vulnerabilidades dos Riscos Identificados**

Esta tarefa tem o propósito de identificar as vulnerabilidades a partir dos riscos e controles identificados. Elas podem estar associadas a diferentes áreas como: organização, processos e procedimentos, rotinas de gerenciamento, recursos humanos, ambiente físico, configuração dos sistemas de informação, hardware, software, entre outras [36]. O template da Figura 5.13 apresenta o modelo para preenchimento das tarefas “Definir controle dos riscos identificados” e "Definir as vulnerabilidades dos riscos identificados":

| IDENTIFICAR CONTROLES | | | | |
|---|---|---|---|---|
| **ID CONTROLE** | **ID RISCO** | DESCRIÇÃO | SITUAÇÃO / JUSTIFICATIVA | VULNERABILIDADE |
| Id1 | Id_risco1 | Descrição1 | Situação1 | Vulnerabilidade1 |

**Figura 5.13:** Template para identificação dos controles e vulnerabilidades. (Fonte: Elaboração própria).

O produto desta tarefa deve ser a documentação das vulnerabilidades levantadas. As informações das vulnerabilidades serão descritas em uma lista com sua descrição e farão parte dos eventos de riscos identificados nas tarefas anteriores.

A partir da análise dos controles documentados, devem ser identificadas, as vulnerabilidades para as quais não há controles implementados. Para cada controle pode haver uma ou mais ameaças relacionadas com vulnerabilidades específicas. Pode ser utilizado um catálogo com vulnerabilidades e controles previamente estabelecidos.

## 5.4 Análise e Avaliação dos Riscos

O processo de análise e avaliação dos riscos compreende a verificação do nível de risco, baseando-se pela combinação da consequência para a organização (impacto) e a chance de ocorrência (probabilidade) dos riscos [34]. A NBR ISO 31000 (2009) descreve que um evento pode ter várias consequências e pode afetar vários objetivos, devendo assim, que os controles existentes e sua eficácia e eficiência também sejam levados em consideração na etapa de análise e avaliação dos riscos [54]. Essa análise e avaliação favorece os gestores de riscos para priorização da implantação do tratamento, auxilia no julgamento se é mais econômico reter um risco ou transferi-lo e na tomada de decisão relacionada aos riscos [16]. O registro da avaliação do risco facilita a monitorização e identificação das prioridades de risco [80].

No processo de análise e avaliação, as ferramentas utilizadas são as de estimativa de probabilidade e impacto dos riscos e a matriz de probabilidade e impacto [13]. A estimativa dos riscos visa compreender o impacto das consequências provocadas caso as

ameaças de fato ocorram, definindo quantitativamente nível de impacto. De maneira geral, trata-se de ponderar as chances de que as ameaças se tornem realidade [36]. A análise e avaliação dos riscos, devem ser baseadas em evidências objetivas, considerando as perspectivas das partes interessadas impactadas pelo risco, que auxiliem na tomada de decisão sobre quais riscos necessitam de tratamento e prioridade para a implantação de tratamentos, fundamentadas em uma etapa de identificação bem realizada [54]. O Quadro 5.4 destaca a estrutura de atividades e tarefas previstas para o processo de análise e avaliação dos riscos da metodologia de gestão de riscos das contratações de TI da FUNASA:

**Quadro 5.4:** Estrutura do processo de análise e avaliação dos riscos. (Fonte: Adaptado de [35, 65, 36, 67]).

| **Análise e Avaliação dos Riscos** | | |
|---|---|---|
| **Atividades** | **Tarefas** | **Fonte** |
| Avaliar Danos e Impactos | Identificar Danos e Consequências | [35] |
| | Definir Impacto dos Riscos | [65] |
| Identificar Probabilidade de Ocorrência | Definir Probabilidades | [36] |
| Estimar Nível de Risco | Definir Estimativa de Riscos | [67] |
| | Avaliar Estimativa de Riscos | [36] |

As atividades e tarefas do processo estão baseadas nas premissas de avaliação dos impactos dos riscos e na definição da probabilidade de ocorrência dos eventos identificados. Para analisar os riscos é necessário compreender os riscos, e as atividades de avaliação de danos e impactos buscam o entendimento do perímetro do risco, indicando onde e o quê o risco influenciará na organização [53]. Para a análise e avaliação dos riscos as entradas, técnicas utilizadas, requisitos do processo e saída esperada descritas na Figura 5.14:

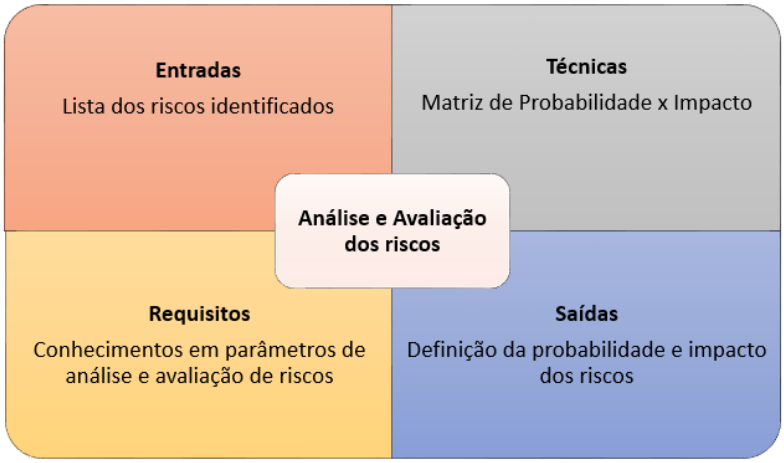


**Figura 5.14:** Processo de análise e avaliação dos riscos: entradas, técnicas, requisitos e saídas. (Fonte: Elaboração própria).

A lista dos riscos identificados é o documento que conduzirá todo estudo de análise e avaliação dos riscos. Outras entradas que poderão ser consideradas, caso necessário, nesse processo como a opinião dos especialistas, que com base na experiência obtida em projetos anteriores, auxilia na determinação do nível de probabilidade e impactos dos riscos [67]. A falta de conhecimento na disciplina de gestão de riscos pode tornar o processo de análise dos riscos incompleto, com dados e parâmetros imprecisos e tornar a prioridade dos riscos invertida, de maneira que os riscos de baixa importância sejam considerados de alta prioridade ou riscos de alta prioridade avaliados como de baixa atenção, por isso, faz-se necessário que a equipe de planejamento obtenha um nivelamento de informações, principalmente quanto à estimativa da probabilidade dos eventos. A norma NBR ISO 31010 (2009) apresenta os fatores que devem ser considerados para seleção das técnicas para o processo de avaliação de riscos [53]:

- Complexidade do problema e os métodos necessários para analisá-lo;
- Natureza e grau de incerteza do processo de avaliação dos riscos, baseado na quantidade de informações disponíveis e o que é requerido para atender os objetivos;
- Extensão dos recursos requeridos e nível de conhecimento especializado;
- Se o método pode fornecer uma saída quantitativa.

Considerando as características do processo de contratação de bens e serviços tecnologia da FUNASA, os riscos identificados não retornarão dados estatísticos, mas na maioria dos casos, dados empíricos dos gestores e da equipe de contratação. Assim, a metodologia proposta irá dispor de técnicas que avaliam qualitativamente os riscos como a matriz de probabilidade e impacto [67].

### 5.4.1 Avaliar Danos e Impactos

A atividade de análise do risco considera a probabilidade do risco ocorrer e o seus possíveis danos e impactos sobre um ou mais objetivos do projeto ou processo finalístico, neste caso, sobre o processo de contratação dos bens e serviços de TI [34]. Esta atividade propõe a avaliação do impacto de riscos investigando o efeito potencial sobre os objetivos da contratação de TI, como cronograma, custo, qualidade ou desempenho, incluindo tanto os efeitos negativos das ameaças como os efeitos positivos das oportunidades [67].

A avaliação dos danos e impactos visa compreender as consequências provocadas caso as ameaças identificadas ocorram de fato e definir um valor quantificado em relação ao nível de impacto. Para isso, contará com as seguintes tarefas:

- Identificar Danos e Consequências;

- Definir Impacto dos Riscos.

### Identificar Danos e Consequências

A norma IN-SLTI/MP 04/2014 descreve que a análise dos riscos das contratações de TI deve mapear os danos potenciais de cada um dos eventos relacionados aos riscos identificados nas atividades de "Identificação dos Riscos que Comprometem o Sucesso da Contratação" e "Identificar Riscos de Não atendimento das Necessidades". Cada risco pode apresentar uma relação causal, na qual um risco pode gerar um ou mais danos e consequências para a instituição e, dessa maneira, a avaliação de suas possíveis causas pode chegar à causa raiz de um risco [35]. A utilização da técnica pode ajudar a equipe de planejamento no relacionamento dos riscos, danos e impactos que devem ser documentados, de acordo com a Figura 5.15:

| ID do Risco | Descrição do Risco | Dano |
|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Área requisitante do bem ou serviço de TI sem condição de prestar um serviço. |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais |

**Figura 5.15:** Template para identificação dos danos e consequências. (Fonte: Elaboração própria).

A premissa por trás da análise causal é que se um erro (ou risco) ocorreu, pode acontecer novamente, a menos que algo seja feito para pará-lo. Assim, aprender com erros do passado evita erros futuros. Para a tarefa em questão, uma boa forma de documenta-la e chegar em bons resultados é a utilização do diagrama de causa e efeito, que é excelente para descobrir as fontes de risco e mapear suas relações. A ferramenta pode produzir uma identificação rápida dos principais danos dos riscos, indicando o efeito (impacto) relacionado, facilitando uma investigação mais aprofundada e levando a uma melhor compreensão do problema.

### Definir Impacto dos Riscos

A significância de um risco pode ser expressa como uma combinação de suas consequências ou impactos nos objetivos do projeto e a probabilidade de tais consequências surgirem. Isto pode ser realizado com escalas qualitativas de consequência ou em uma matriz que define o significado de várias combinações destes [16].

A tarefa objetiva analisar o impacto das possíveis consequências de riscos quando as ameaças se tornam realidade e provocam danos na organização. Essa perspectiva deve ser feita de maneira ampla no projeto, englobando cada ameaça para a contratação de TI em questão. A equipe de planejamento deve gerar uma análise que reflita a extensão do dano causado pela perda possível ao projeto ou à outras áreas, processos, ações e objetivos institucionais. Para isso, devem ser levados em consideração impactos diretos e indiretos, custos adicionais e o comprometimento da imagem da organização [36]. A Figura 5.16 apresenta as informações que devem ser consideradas nesta tarefa:

| ID do Risco | Descrição do Risco | Impacto | Tipo do Impacto | Nível |
|---|---|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Paralisação de serviços. | Alto |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Paralisação de serviços. | Alto |

**Figura 5.16:** Template para análise dos impactos. (Fonte: Elaboração própria).

Para o *Institute of Risk Management* a análise do impacto deve considerar níveis diferentes para cada consequência do risco em questão, assim, o impacto deve ser descrito de acordo com a medida abaixo [65]:

**Alto:** O processo de contratação não terá o resultado esperado, o risco pode gerar alto impacto na organização, seja financeiro, estratégico ou nas atividades operacionais, traz preocupação significativa das partes interessadas, pode paralisar ações da instituição;

**Médio:** O processo irá piorar no decorrer da contratação, o impacto do risco é considerável no nível estratégico, financeiro ou nas atividades operacionais da organização com preocupação moderada das partes interessadas, não paralisam as ações da instituição;

**Baixo:** Impactos financeiros, estratégicos, operacionais de baixa consequência, trazem estado de atenção aos interessados, mas não inviabilizam o projeto de contratação de TI.

A equipe de contratação, responsável pela tarefa, considerando as fontes de riscos identificadas na tarefa "Identificação das fontes de riscos e áreas de impacto", deve listar possíveis tipos de consequências, informações históricas (considerando inclusive incidentes que ocorreram) e o conhecimentos dos envolvidos em outras contratações de TI finalizadas.

Pode-se considerar categorizar os impactos para que, em futuras contratações, sejam de fácil levantamento os impactos do projeto, como no exemplo das categorias de impacto: prejuízo financeiro, paralisação de serviços, violação jurídica, danos materiais entre outros [36].

O resultado dessa atividade complementa a identificação dos impactos da fase de identificação dos riscos, com as informações de tipo e sua descrição mais completa, classificando o impacto para cada risco, detalhando as consequências do risco para a organização, para outras áreas e para outros ativos da organização. Caso haja prejuízo financeiro deve ser documentado referenciando valores.

### 5.4.2 Identificar Probabilidade de Ocorrência

A NBR ISO 31000 (2009) estabelece que a análise de riscos envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas e a probabilidade de que essas consequências possam ocorrer [54]. A atividade de identificação da probabilidade de ocorrência deve calcular a possibilidade de cada um dos eventos relacionados a cada risco identificado nas atividades anteriores e apresentar a relação risco e probabilidade [35]. A determinação da probabilidade expressa o nível de cada risco identificado, que combinado com as consequências mapeadas irão determinar quais riscos devem ter maior atenção, tratamentos prioritários e respostas ágeis da instituição.

A avaliação de probabilidade deve refletir a frequência que a ameaça pode ocorrer e como as vulnerabilidades são exploradas. A atividade de identificação da probabilidade no processo de gestão dos riscos, busca avaliar dois acontecimentos: a probabilidade de um evento de ameaça ser provocado ou ocorra de maneira acidental aleatória; ou ainda, que após um evento de ameaça iniciado, resulte em impactos diversos na instituição [36]. Para a atividade de identificação de probabilidade de ocorrência dos riscos será necessária a execução da tarefa de definição de probabilidades.

#### Definir Probabilidades

As probabilidades dos riscos podem ser determinadas a partir de uma modelagem dos resultados de um evento ou conjunto de eventos, ou a partir de estudos experimentais com os dados disponíveis [54]. A equipe de contratação de TI deve avaliar as probabilidades dos riscos identificados a partir da avaliação dos impactos e ameaças levantadas, considerando a possibilidade dos eventos se concretizarem, provocando assim danos à organização, a partir de uma escala definida no Quadro 5.5 pelo *Institute of Risk Management* como [65]:

**Quadro 5.5:** Tabela de probabilidade de ocorrência. (Fonte: [65]).

| Escala | Descrição |
|---|---|
| Alta (Provável) | Grande possibilidade de ocorrência, maior que 75%. |
| Média (Possível) | Perspectivas razoáveis de resultados favoráveis entre 25% e 75%. |
| Baixa (Remota) | Existe alguma chance de ocorrência com chances abaixo de 25%. |

A avaliação da probabilidade de ocorrência de um risco ou oportunidade, requer a compreensão que a escala deslizante vai de 0 a 100. Se não houver chance de um evento acontecer, há uma probabilidade de zero, caso o evento seja inevitável tem-se uma probabilidade de 100%, para cada risco a equipe de contratação deve analisar a possibilidade da ameaça se materializar, definindo a probabilidade a partir da escala definida no Quadro 5.5 [16]. Para a finalização desta tarefa, o quadro dos riscos identificados deve ser atualizado de acordo com a Figura 5.17 do template:

| ID do Risco | Descrição do Risco | Ameaças | Impactos | Probabilidade |
|---|---|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Operacionalidade das áreas fim prejudicada, atraso em atender a sociedade. | Médio |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Área fim sem material para executar suas tarefas. | Alto |

**Figura 5.17:** Template para avaliação de probabilidade dos riscos. (Fonte: Elaboração própria).

A avaliação de probabilidade poderá ser feita utilizando técnicas de reuniões e matrizes de probabilidade e impacto [67]. Para cada risco deve ser identificada a classe de probabilidade – Baixa (B); Média (M); Alta (A), além das justificativas para classificação, consultando se necessário, o gestor da área de TI e a opinião dos especialistas nos projetos de contratação de TI do órgão, considerando a experiência sobre projetos anteriores e informações históricas de incidentes em outros projetos. Essa consulta pode apresentar uma classificação mais realista que gere um plano de tratamento dos riscos eficaz.

### 5.4.3 Estimar Nível de Risco

Com a avaliação de probabilidade, os riscos poderão diferir em nível de urgência, variando sua complexidade, importância e o tempo de antecedência com que precisam ser tratados e também ao tempo necessário para respostas. Riscos com a mesma probabilidade e impacto

podem ter níveis de urgência de tratamento diferentes. A atividade de estimativa dos riscos visa obter um nível que considere conjuntamente os impactos e as probabilidades, chegando à um nível de gravidade dos riscos [34].

Esse nível de relacionamento entre probabilidade e impacto a literatura chama de apetite do risco, que é a quantidade de risco que a organização está preparada para aceitar, tolerar ou estar exposta. O apetite ao risco é fundamental para o gerenciamento eficaz dos riscos, podendo variar de acordo com os objetivos da organização sendo útil para estabelecer objetivos claros ao se gerenciar os riscos [16].

Um risco pode ser considerado aceitável no nível estratégico, mas inaceitável entre os membros da equipe de contratação de TI, por isso nesta etapa é necessário considerar a participação dos gestores estratégicos da organização, como de TI e autoridade administrativa competente, definindo o nível de exposição que é considerado aceitável em termos de impacto tolerável e a frequência tolerável deste impacto. Podemos definir o nível de riscos que a organização está disposta a tolerar para um determinado projeto de contratação de TI, utilizando o conceito de tolerância a riscos, que se excedido, deverá ser reportado e uma ação específica deve ser tomada. Para esta atividade, a equipe de contratação conduzirá as tarefas de definição e avaliação da estimativa de riscos [34].

### Definir Estimativa de Riscos

As classificações dos riscos são designadas com base na avaliação da sua probabilidade e impacto. A avaliação da importância de cada risco e a prioridade é conduzida usando uma matriz de probabilidade e impacto de referência, de acordo com a definida na Figura 5.18, baseada no *Orange Book* do governo britânico, que verifica o nível de priorização dos riscos para uma posterior análise das respostas [67].

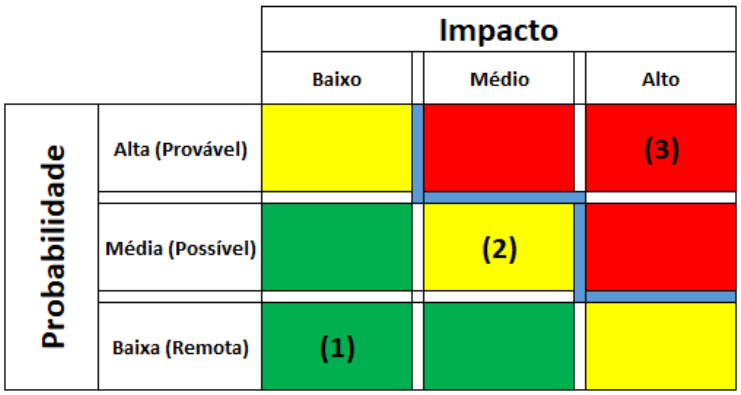


**Figura 5.18:** Matriz de Probabilidade Impacto. (Fonte: Adaptado de [80]).

Cada risco identificado será analisado de acordo com sua probabilidade de ocorrência e seu impacto nos objetivos da contratação de TI da FUNASA, sendo posicionado no quadrante respectivo da matriz, com as combinações de probabilidade e impacto em uma classificação de alto risco, risco moderado e baixo risco. A respectiva matriz em verde, amarelo e vermelho, indica as condições dos riscos pelas diferentes cores, demonstrando seu grau de tolerância e o tratamento que deve ser observado [34].

Na Figura 5.18, os riscos situados nas áreas (1) verde, (2) amarela ou (3) vermelha da matriz, representam a definição da faixa de valores dos níveis de riscos. A faixa de valores é definida pela seguinte estrutura [67]:

**(1) Alto risco:** risco intolerável, ameaça de grande preocupação, ações imediatas devem ser tomadas e os resultados precisam ser monitorados frequentemente;

**(2) Risco moderado:** situação de atenção, risco pode ser tratado em médio prazo e monitorado frequentemente;

**(3) Baixo risco:** risco tolerável, não necessita de ação imediata, porém o risco deve ser monitorado.

A área demarcada pela linha de cor azul representa o nível de tolerância aos riscos, exigindo que sejam reportados e que autorizações e ações específicas devam ser demandadas. O nível de tolerância a riscos, expresso pela linha de tolerância, indica que a organização aceitará ou responderá por essas ameaças com tratamento específico não podendo ser aceitos sem que sejam autorizados por nível de autoridade superior. Após o término desta tarefa, o quadro dos riscos deve conter as devidas estimativas informadas, de acordo com o template da Figura 5.19:

| ID do Risco | Descrição do Risco | Ameaças | Nível do Impacto | Probabilidade | Nível de Risco |
|---|---|---|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Alto | Médio | Alto risco |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Alto | Alto | Alto risco |

**Figura 5.19:** Template para definição da estimativa dos riscos. (Fonte: Elaboração própria).

Para cada risco identificado, no artefato deverá apresentar a descrição do risco, as ameaças relacionadas, nível do impacto, probabilidade de ocorrência e nível do risco (relação de probabilidade e impacto de acordo com a matriz apresentada acima).

**Avaliar Estimativa de Riscos**

Após a análise da estimativa dos riscos, o gestor de TI verifica as informações das estimativas de riscos no quadro de riscos gerados na tarefa anterior e, caso esteja de acordo, deve aprová-los, caso o risco necessite de aprovação por autoridade superior competente, deve ser enviado para a avaliação e posterior aprovação. Caso estejam de acordo, o gestor de TI e a autoridade competente devem registrar a aprovação e encerram-se dessa forma, as atividades do processo de análise e avaliação dos riscos. Caso contrário, o gestor deve notificar a equipe de contratação de TI, para a necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações [36].

Neste ponto da metodologia de gestão de riscos das contratações de TI da FUNASA, já será possível uma visão mais clara de quais ameaças existem para o projeto de contratação de TI do órgão e o quanto este projeto estará ou não protegido por meio de controles. Nesta tarefa ainda é possível a classificação de riscos, com a criação de uma lista ordenada dos riscos e seu nível de urgência avaliado. Isso permite distinguir os riscos mais relevantes do projeto como um todo, além de ser uma base para as decisões sobre quais riscos devem ser tratados prioritariamente [65].

Os resultados da etapa de análise e avaliação de riscos devem ser registrados de maneira que todas as etapas do processo sejam documentadas e complemente as informações inseridas como resultado da etapa anterior de identificação dos riscos. As informações dessa etapa devem conter elementos como: probabilidade do evento de risco e descrição da probabilidade; impacto do evento de risco e descrição do impacto; nível de risco (combinação probabilidade e impacto); matriz de probabilidade e impacto; data da análise; e nível de urgência dos riscos.

## 5.5 Tratamento dos Riscos

O tratamento dos riscos é a etapa de selecionar e implementar medidas para modificar o risco, isto inclui, o controle, a mitigação, a prevenção e a transferência do risco. A partir do quadro dos riscos identificados e devidamente analisados, a presente etapa direcionará decisões sobre o tratamento de riscos [65]. O PMBOK (2013) descreve que o planejamento das respostas aos riscos é um processo de desenvolvimento de opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos do projeto, com a vantagem da

abordagem dos riscos por prioridades, investindo recursos e atividades nos riscos mais estratégicos [67]. O tratamento de riscos envolve a tomada de decisão estratégica sobre uma ou mais opções de tratamento em um processo cíclico que avalie o tratamento de riscos já realizados, decida se os níveis de risco são toleráveis e a sua avaliação eficaz do tratamento dos riscos [54].

A norma ABNT NBR ISO 31000 (2009) descreve que as opções de tratamento de riscos não são necessariamente adequadas em todas as circunstâncias, devendo verificar risco a risco a aplicação necessária dos controles [54]. O *Orange Book* apresenta as seguintes opções para o tratamento dos riscos [80]:

**Mitigar:** O objetivo desta ação é que, mesmo continuando com a iniciativa que deu origem ao risco, a organização tome a ação de controle para conter o risco em um determinado nível. Implicando em redução da probabilidade e/ou impacto de um evento de risco para dentro de limites aceitáveis;

**Transferir:** A transferência de riscos também pode ser considerada para transferir o nível de exposição da organização ou porque outra organização é mais capaz de gerenciar o risco. Alguns riscos não são totalmente transferíveis, pois o relacionamento com o terceiro para o qual o risco foi transferido deve ser muito bem gerenciado para assegurar a transferência do risco;

**Eliminar:** Alguns riscos podem ser tratados somente pela alteração de objetivos via redução de escopo, alteração de requisitos e cronograma até término da atividade ou projeto;

**Aceitar:** A exposição ao risco é tolerada sem que nenhuma ação específica seja tomada. Mesmo se o risco não for tolerável, a capacidade para fazer alguma coisa com relação ao risco pode ser limitada, ou o custo de tomar uma ação pode ser desproporcional ao benefício potencial gerado. Nesses casos, a resposta pode ser tolerar o nível de risco. Esta opção, é claro, pode ser suplementada por um plano de contingência para conter os impactos que adviriam caso a ameaça ocorra.

O tratamento dos riscos envolve selecionar a maneira adequada para controlar o risco, com o devido equilíbrio entre os custos e esforços para implementação e as limitações impostas para uma resposta eficaz ao risco. As atividades e tarefas consideradas para a metodologia envolvem a combinação de vários fatores, de forma a atender as percepções e valores da FUNASA e estão estruturadas de acordo com o Quadro 5.6:

**Quadro 5.6:** Estrutura do processo de tratamento dos riscos. (Fonte: Adaptado de [67, 80, 36]).

| **Tratamento dos Riscos** | | |
|---|---|---|
| **Atividades** | **Tarefas** | **Fonte** |
| Planejar Respostas aos Riscos | Definir Plano de Tratamento dos Riscos | [67] |
| | Definir Estratégia de Respostas para os Riscos | [80] |
| Definir Ações de Prevenção | Definir Tratamento e Ações de Contingência para Prevenção dos Riscos | [36] |

As atividades e tarefas do processo de tratamento de riscos devem apresentar mecanismos para o devido controle dos riscos que darão efetividade à gestão de riscos elaborada até o momento. Assim, as ações devem analisar se o plano de resposta aos riscos está surtindo o efeito desejado dentro do menor custo para a organização. As entradas, ferramentas e técnicas, saídas e requisitos do processo são descritas na Figura 5.20 [16]:

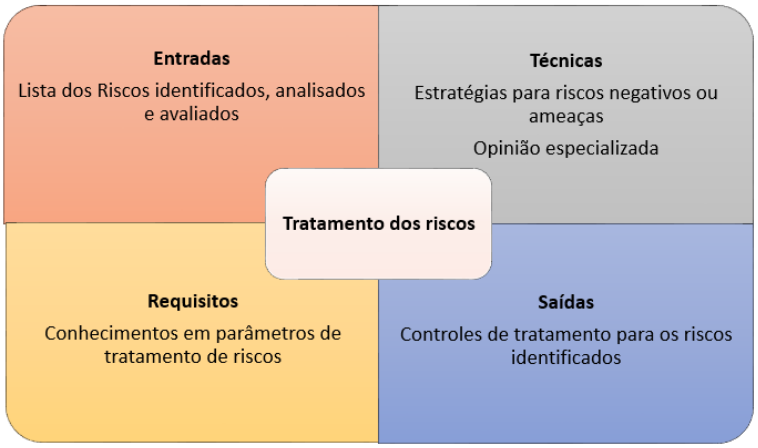


**Figura 5.20:** Processo de tratamento dos riscos: entradas, técnicas, requisitos e saídas. (Fonte: Elaboração própria).

Os riscos identificados e analisados nas atividades anteriores são insumos no processo de tratamento dos riscos. Os registros dos riscos são desenvolvidos incrementalmente ao longo dos processos anteriores. Cada risco identificado terá seu devido planejamento de resposta, criando assim um banco de dados de risco também para os controles e tratamentos estabelecidos. As atualizações ou registro dos controles, com o respectivo documento do plano de ação ou artefato de tratamento dos riscos, são os resultados do processo de tratamento dos riscos. Alguns indicadores de desempenho podem ser utilizados, como a verificação das ações corretivas e sua efetividade no objetivo dos controles e andamento no cronograma do projeto.

O conhecimento em gestão de riscos, nos projetos de contratação de TI, é um requisito para a etapa de tratamento dos riscos, pois trará empenho e assertividade aos controles estabelecidos. A falta de conhecimento pode gerar ações ineficazes. As técnicas e ferra-

mentas utilizadas para o tratamento dos riscos, vão do estabelecimento do plano de ação com a utilização de estratégias para as ameaças, respostas e controles dos riscos, até a opinião dos especialistas em relação aos riscos e seus impactos [16].

### 5.5.1 Planejar Respostas aos Riscos

Após a análise dos riscos identificados, deve-se planejar as respostas para os riscos considerando as restrições que potencialmente podem afetar as decisões sobre o tratamento de riscos, como custos, prazos, entre outros. Nesse sentido, os riscos podem passar por uma análise preliminar a fim de estimar os custos, esforço e prazo e se existem restrições para o tratamento do risco [36]. As respostas planejadas trarão eficácia de custos para atender ao desafio, ser realistas dentro do contexto do projeto, acordadas por todas as partes envolvidas e ter um responsável designado. Em geral é necessário selecionar a melhor resposta ao risco entre as diversas opções possíveis. Caso as restrições de custo, esforço e prazo não sejam significativas para a tomada de decisão, esta atividade pode ser suprimida [67].

Para cada risco identificado, devem ser recuperadas as informações levantadas nas atividades anteriores como dos controles identificados na atividade "Identificar Controles e Vulnerabilidades", atualizando para cada controle, a situação de sua implementação. Deve ser feita uma estimativa do custo, esforço e de prazo para implementar os controles identificados e com a situação de “Não implementado”. Nesta atividade os controles, terão sua implementação planejada, para reduzir a exposição da contratação de TI ao risco.

#### Definir Plano de Tratamento dos Riscos

O plano de tratamento dos riscos será elaborado considerando os componentes de custo, esforço, tempo e limites para tolerância dos riscos. Os limites ajudam a identificar os riscos para os quais são necessárias respostas específicas. Para isso, deve ser elaborado um cronograma com os riscos que exigem respostas e o prazo para as respostas e a lista de riscos em observação, que devem ser monitorados mas possuem baixa prioridade dentro do registro dos riscos, de acordo com a Figura 5.21 [67]:

| Nível do Risco | ID | Risco | Prazo para Resposta | Observação |
|---|---|---|---|---|
| Alto risco | 01 | Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda às necessidades do órgão. | 30/05/2017 | |
| | 02 | Sobrecarga dos servidores responsáveis por atividades do processo de gestão de contratos. | 01/07/2017 | |
| | 03 | Falta de servidores na área de TI com domínio do processo de gestão contratual. | 30/07/2017 | |
| | 04 | Contratação com partes faltantes ou solução incompleta. | 01/08/2017 | |
| Risco moderado | 05 | Atraso do início dos trabalhos da contratada devido ao órgão não oferecer as condições necessárias para inícios dos trabalhos. | Finalização do processo de contratação | Monitorar até a conclusão. |
| | 06 | Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação de TI. | Finalização do processo de contratação | Monitorar até a conclusão. |
| | 07 | Coleta insuficiente de preços, levando a estimativa inadequadas. | Finalização do estudo técnico preliminar. | Monitorar até a conclusão. |
| | 08 | Utilização de somente uma solução do mercado como base para a definição de requisitos, levando ao direcionamento. | Finalização do estudo técnico preliminar. | Monitorar até a conclusão. |
| | 09 | Falta de passagem de conhecimento entre fornecedor e o órgão. | Finalização do contrato | Monitorar |

**Figura 5.21:** Cronograma de respostas dos riscos mais críticos. (Fonte: Elaboração própria).

A tarefa será de responsabilidade da equipe de contratação que deve, com apoio dos gestores, estimar, os custos de implementação dos controles para tratar cada risco, o quanto de esforço é necessário para implementar cada controle definido identificando as devidas restrições que impactem na escolha do tratamento do risco. A tarefa deve retornar as seguintes informações de acordo com o template da Figura 5.22:

| ID do Risco | Descrição do Risco | Nível de Risco | Controles | Estimativa para implementação | | | Restrições |
|---|---|---|---|---|---|---|---|
| | | | | Custo | Prazo | Esforço | |
| 01 | Coleta insuficiente de preços, levando a estimativas de preços sem o devido embasamento. | Alto risco | A equipe de planejamento deve consultar diversas fontes para obter preços a serem usados nas estimativas de preço da contratação de TI. | Custos relativos à telefone, internet e correio. | 3 meses | Nome1, Nome2, Nome3 | Sem restrições |
| | | | A equipe de contratação deve utilizar índices para ajustar os preços obtidos diretamente com os fornecedores. | Custos relativos à telefone, internet e correio. | 1 mês | Nome1, Nome2, Nome3 | Sem restrições |
| | | | Elaborar memória de cálculo das estimativas de preço, anexando evidências das pesquisas realizadas. | Custos com impressão | 3 meses | Nome1, Nome2, Nome3 | Sem restrições |

**Figura 5.22:** Template para definição do plano de tratamento dos riscos. (Fonte: Elaboração própria).

Devem ser considerada a disponibilidade de recursos humanos para realizar os tratamentos dos riscos analisados. Posteriormente, a equipe de contratação deve notificar o gestor de TI ou autoridade responsável, para validação das informações levantadas.

**Definir Estratégia de Respostas para os Riscos**

As respostas para os riscos identificados devem ser elaboradas a partir da seleção da estratégia que a FUNASA irá tomar para as ações de tratamento. As estratégias descritas anteriormente para a resposta aos riscos da metodologia de gestão de riscos das contratações de TI da FUNASA são: mitigar, transferir, eliminar, aceitar. Dessas opções, três estratégias lidam com ameaças ou riscos que podem ter impactos negativos nos objetivos da contratação de TI, se ocorrerem, são eliminar, transferir e mitigar. A estratégia aceitar, pode ser usada para riscos negativos ou ameaças quanto para riscos positivos ou oportunidades.

Cada uma dessas estratégias de resposta ao risco tem uma influência nos objetivos das ações que tratarão os riscos. Essas estratégias devem ser escolhidas para cada risco identificado e corresponder à probabilidade e impacto do risco nos objetivos da contratação. As opções de eliminar e mitigar os riscos são, geralmente, para riscos críticos, enquanto aceitar e transferir são para ameaças de menor impacto no projeto [67].

Os integrantes da equipe de contratação, a partir do documento com os riscos analisados, deve informar risco a risco qual será a opção de tratamento para respectiva contratação de TI (mitigar, transferir, eliminar, aceitar).

### 5.5.2 Definir Ações de Prevenção

A ações de prevenção devem analisar cada risco e seu respectivo nível de risco e estabelecer o plano de ação recomendado de acordo com planejado na tarefa "Definir Plano de Tratamento dos Riscos". Nesta atividade, a equipe de planejamento da contratação definirá as ações a serem tomadas para reduzir ou eliminar as chances de ocorrência dos eventos relacionados aos riscos identificados nas atividades anteriores, bem como sua respectiva periodicidade de monitoramento [35].

As ações serão esquematizadas para serem usadas somente se certos eventos ocorrerem. Para alguns riscos, que demandem mais tempo e recursos, é apropriado que a equipe de planejamento desenvolva um plano de ação das respostas que deve ser executado sob determinadas condições predefinidas, caso acredite-se que haverá alerta suficiente para implementar o plano. Os eventos para as respostas de contingência, devem ser definidos e acompanhados. O PMBOK (2013) descreve que essa técnica de respostas aos riscos identificados, são muitas vezes chamadas de planos de contingência ou planos alternativos, e incluem eventos geradores identificados que colocam os planos em vigor. Outra importante técnica definida pelo PMBOK para essa atividade é a opinião especializada fornecida por pessoas experientes em relação às ações a serem adotadas para um risco específico e definido. A opinião especializada deve ser orientada para os grupos ou pessoas

com formação especializada, conhecimentos, habilidade, experiência ou treinamento em definição de respostas à riscos [67].

### Definir Tratamento e Ações de Contingência para Prevenção dos Riscos

Depois de finalizadas as tarefas de "Definir Plano de Tratamento dos Riscos" e "Definir Estratégia de Respostas para os Riscos", devem ser realizadas as decisões sobre quais ações irão tratar os riscos. Esta decisão deve considerar os riscos priorizados (alto risco, risco moderado e baixo risco), as opções de tratamento (mitigar, transferir, eliminar e aceitar) e as estimativas feitas para a implementação dos controles (custo, esforço, tempo e restrições).

A condição para a etapa ser finalizada é que todos os riscos tenham sua opção de tratamento selecionada, com o devido responsável atribuído e a tarefa, deve retornar as seguintes informações de acordo com o template da Figura 5.23:

| ID do Risco | Descrição do Risco | Nível de Risco | Controles | Estimativa para implementação | | | Restrições | Opção para Tratamento | Ações de Prevenção | Responsável |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Custo | Prazo | Esforço | | | | |
| xx | Coleta insuficiente de preços, levando a estimativas de preços sem o devido embasamento. | Alto risco | A equipe de planejamento deve consultar diversas fontes para obter preços a serem usados nas estimativas de preço da contratação de TI. | Custos relativos à telefone, internet e correio. | 3 meses | Nome1, Nome2, Nome3 | Sem restrições | Eliminar | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |
| | | | A equipe de contratação deve utilizar índices para ajustar os preços obtidos diretamente com os fornecedores. | Custos relativos à telefone, internet e correio. | 1 mês | Nome1, Nome2, Nome3 | Sem restrições | Mitigar | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |
| | | | Elaborar memória de cálculo das estimativas de preço, anexando evidências das pesquisas realizadas. | Custos com impressão | 3 meses | Nome1, Nome2, Nome3 | Sem restrições | Transferir | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |

**Figura 5.23:** Template para definição do tratamento dos riscos. (Fonte: Elaboração própria).

Os riscos serão analisados um por vez, estabelecendo um plano de ação para cada respectivo risco. Deverão ser definidas as ações que devem ser tomadas para remediar o impacto da ocorrência do evento relacionado ao risco identificado. Isto vai considerar ações de prevenção para os riscos e ações de contingência. Esta tarefa definirá o tratamento para a prevenção do risco. O primeiro passo é analisar se os controles identificados anteriormente possuem algum estado de implementação (Não implementado; Parcialmente implementado; Totalmente implementado; Não se aplica; ou Desnecessário) e com auxílio das estimativas feitas na tarefa "Definir Plano de Tratamento dos Riscos", a equipe de planejamento descreverá as ações que devem ser realizadas para cada controle, estabelecendo ainda os responsáveis por cada ação.

## 5.6 Monitorar e Controlar os Riscos

Para que a metodologia de gestão de riscos das contratações de TI da FUNASA seja eficaz é necessária uma estrutura de relatórios e revisão para que as ações previstas na etapa de tratamento de riscos sejam efetivamente aplicadas aos riscos identificados. As organizações são dinâmicas e operam em ambientes dinâmicos e por isso, o desempenho da gestão de riscos deve ser acompanhado para identificar oportunidades de melhoria [65].

A norma ABNT NBR ISO 31010 (2009) descreve que os riscos e controles devem ser regulamente monitorados com uma análise crítica para verificar que [53]:

- As premissas sobre os riscos permanecem válidas;
- As premissas nas quais o processo de avaliação de riscos é baseado permanecem válidas;
- Os resultados esperados estão sendo alcançados;
- Os resultados do processo de avaliação de riscos estão alinhados com a experiência corrente;
- As técnicas do processo de avaliação de riscos estão sendo aplicadas de maneira apropriada;
- Os tratamentos de risco são eficazes.

O PMBOK (2013) apresenta que *controlar os riscos é o processo de implementação de planos de respostas aos riscos, acompanhamento dos riscos identificados, monitoramento dos riscos residuais, identificação de novos riscos e avaliação da eficácia do processo de riscos durante todo o projeto.* Monitorar e controlar os riscos melhoram a eficiência da gestão de riscos otimizando sua execução [67]. O controle não é uma atividade neutra, e não deve ser uma cópia do que foi aplicado em atividades anteriores. Controlar requer intervenção, utilização das informações recolhidas do acompanhamento para satisfazer os objetivos [16]. Outro fato importante ao monitorar e controlar os riscos é analisar os eventos, mudanças, tendências, sucessos e fracassos da gestão de riscos para aprender com eles [54].

A etapa de monitoração e controle da gestão de riscos, deve utilizar indicadores, os quais devem ser analisados criticamente, de forma periódica, para garantir sua adequação, medindo o progresso obtido, analisando as mudanças organizacionais [54]. Além disso monitorar os eventos de riscos está relacionado à comunicação que todo processo deve possuir com os envolvidos na gestão de riscos. A comunicação se desenvolve simultaneamente com os demais processos e as atividades que são executadas durante todo o processo de

gestão de riscos. Para a metodologia proposta, o processo Monitorar e Controlar os riscos compreenderá as seguintes atividades e tarefas, contidas no Quadro 5.7:

**Quadro 5.7:** Estrutura do processo monitorar e controlar os riscos. (Fonte: Adaptado de [67, 5]).

| Monitorar e Controlar os Riscos | | |
|---|---|---|
| **Atividades** | **Tarefas** | **Fonte** |
| Gerar Relatórios de Acompanhamento | Elaborar Relatório de Controle dos Riscos | [67] |
| Definir Plano de Comunicação | Elaborar Plano de Comunicações de Riscos | [5] |

Convém que as atividades e tarefas do processo de monitoramento e controle dos riscos abranjam todos os aspectos do processo da gestão de riscos com a finalidade de garantir que os controles sejam eficazes e eficientes no projeto e na operação, obter informações adicionais para melhorar o processo de avaliação dos riscos, analisar o ambiente e suas mudanças ou tendências e aprender com eles e identificar novos riscos que surjam durante a gestão dos riscos [54]. O processo para monitorar e controlar os riscos apresenta as entradas, técnicas utilizadas, requisitos do processo e saída esperada descritas na Figura 5.24:

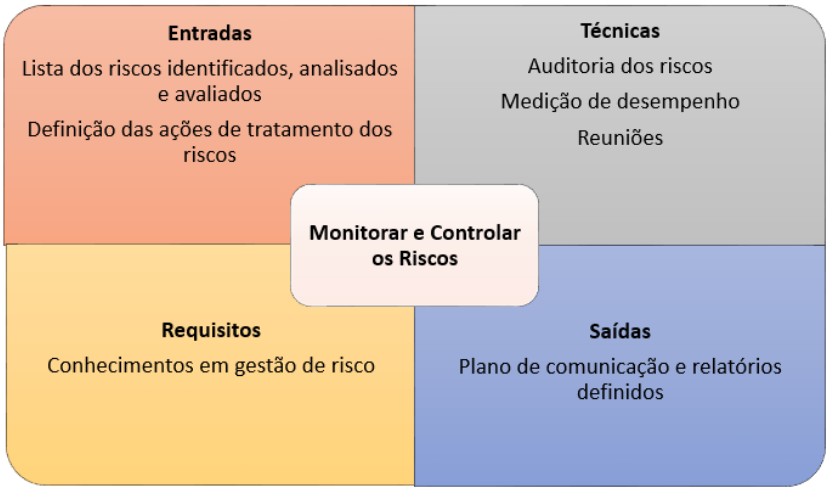


**Figura 5.24:** Processo de monitoração e controle dos riscos: entradas, técnicas, requisitos e saídas. (Fonte: Elaboração própria).

### 5.6.1 Gerar Relatórios de Acompanhamento

Para se obter um controle eficaz durante a gestão de riscos das contratações de TI da FUNASA, é necessário um programa proativo que monitore regularmente os riscos e o status dos riscos identificados. Deve ser definida uma estratégia com os intervalos e o

status de risco que deve ser revisitado. Esta atividade pode resultar na descoberta de novos riscos ou em novas opções de tratamento de risco que possam exigir replanejamento e reavaliação. Este acompanhamento inclui a elaboração de relatórios e reuniões regulares. Cada relatório fornecerá um risco e uma oportunidade status, registrando o progresso (ou falta dele) feito contra as ações atribuídas a cada risco e oportunidade. Dados de eventos ou perdas, causa raiz dos eventos de perda e opções para mitigar riscos (custos e benefícios) [77].

Esta atividade deve retornar informações que tragam ao gestor de TI um panorama dos riscos da contratação de TI em questão, e deve apresentar informações como [77]:

- Listas atualizadas de status de risco;
- Avaliações atualizadas da probabilidade dos riscos;
- Lista atualizada de opções de tratamento de riscos;
- Lista atualizada das ações para lidar com os riscos.

#### Elaborar Relatório de Controle dos Riscos

A equipe de planejamento da contratação deve avaliar periodicamente a execução da gestão de riscos, verificando a evolução dos controles, status, probabilidade e tratamento dos riscos, registrando o progresso da implementação (em percentual realizado).

A elaboração dos relatórios pode ser realizada a partir de reuniões definidas pela tarefa de "Definição do ciclo de acompanhamento e revisão", na qual os envolvidos, a partir da lista do riscos identificados e do cronograma de tratamento dos riscos estabelecido na tarefa "Definir Plano de Tratamento dos Riscos", irá revisar as ações de tratamento atualizando o campo de status e progresso. A equipe de contratação poderá utilizar as técnicas de medição de desempenho e auditoria de riscos que examinam e documentam a eficácia das respostas para lidar com os riscos identificados e suas causas principais, bem como a eficácia do processo de gestão dos riscos [67].

Ao final da tarefa a equipe de contratação ou responsável pela geração do relatório deve avaliar a correção dos controles estabelecidos e fornecer uma descrição sobre as ações realizadas. O template da Figura 5.25 apresenta as informações que devem ser retornadas desta tarefa:

| Nível do Risco | ID | Risco | Ações de Tratamento | Progresso de Implantação | Status Implementação | Prazo para Resposta | Observação |
|---|---|---|---|---|---|---|---|
| Alto risco | 01 | Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda às necessidades do órgão. | Ação1 | 100% | Implementado | 30/05/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 100% | Implementado | | |
| | 02 | Sobrecarga dos servidores responsáveis por atividades do processo de gestão de contratos. | Ação1 | 10% | Incompleto | 01/07/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 100% | Implementado | | |
| | 03 | Falta de servidores na área de TI com domínio do processo de gestão contratual. | Ação1 | 10% | Incompleto | 30/07/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 100% | Implementado | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 04 | Contratação com partes faltantes ou solução incompleta. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| Risco moderado | 05 | Atraso do início dos trabalhos da contratada devido ao órgão não oferecer as condições necessárias para inícios dos trabalhos. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 06 | Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação de TI. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 07 | Coleta insuficiente de preços, levando a estimativa inadequadas. | Ação1 | 100% | Implementado | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 100% | Implementado | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 08 | Utilização de somente uma solução do mercado como base para a definição de requisitos, levando ao direcionamento. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 09 | Falta de passagem de conhecimento entre fornecedor e o órgão. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |

**Figura 5.25:** Template para relatório de controle dos riscos. (Fonte: Elaboração própria).

As informações referentes ao relatório de controle dos riscos auxiliarão a equipe de planejamento para tornar a gestão de riscos eficaz, avaliando os resultados dos controles e do tratamento estabelecidos, tal percepção deve ser compartilhada com os gestores para aperfeiçoamento da metodologia proposta.

### 5.6.2 Definir Plano de Comunicação

A comunicação de risco é uma parte chave neste processo, na qual as pessoas comunicarão sobre questões, incidentes e evolução do processo de gestão de riscos. A comunicação desequilibrada com um projeto em risco, especialmente em casos de alto risco, pode levar a uma percepção incorreta sobre o risco real por parte de terceiros, como clientes, investidores ou reguladores [5]. Um processo de gerenciamento de riscos adequado, que utilize um bom plano de comunicação, reduz as chances de surpresas para os gestores, da ciência de um risco somente depois que ele se transformou em crise [34]. Os benefícios da comunicação para a gestão de risco incluem [5]:

- Contribuir para a compreensão da gestão executiva da exposição real ao risco de TI, permitindo a definição de respostas de risco adequadas e informadas;

- Sensibilização de todas as partes interessadas internas sobre a importância de integrar o risco e a oportunidade nas suas tarefas diárias;
- Transparência para as partes interessadas externas sobre o nível real dos processos de gestão de risco e de risco em uso.

### Elaborar Plano de Comunicações de Riscos

A comunicação do risco é importante para um bom entendimento dos riscos e para decidir quais as ações a serem tomadas. Esta tarefa trata da comunicação dos riscos entre os envolvidos no processo de gestão de riscos do processo de contratação de TI da FUNASA. Tem por objetivo comunicar o desenvolvimento das atividades e os resultados alcançados em todas as fases da gestão de riscos. Esta tarefa se desenvolve simultaneamente com as demais atividades e tarefas e deve ser executada durante todo o processo de gestão de riscos. [36]. Os dados que conterão o plano de comunicação da metodologia de gestão de riscos das contratações de TI da FUNASA poderão seguir o template 5.26:

| PLANO DE COMUNICAÇÃO DE RISCOS | | | | | | |
|---|---|---|---|---|---|---|
| **ID** | Evento | Informação | Periodicidade | Forma de Comunicação | Responsável | Parte Interessada |
| **01** | Incidente | Risco | Mensal | Email | Equipe de contratação | Área demandante da solução |

**Figura 5.26:** Template para elaboração do plano de comunicações dos riscos. (Fonte: Elaboração própria).

A equipe de contratação de posse de todas as informações anteriores levantadas como: objetivos da contratação, escopo, partes interessadas envolvidas, ciclo de acompanhamento, conhecimento dos profissionais, responsáveis pelas áreas de impacto, responsáveis pelos controles e ações de prevenção dos riscos, deve elaborar o plano de comunicação de riscos, definindo o público-alvo que será comunicado, o tempo apropriado de entrega para cada informação, os resultados desejados, a forma como a informação será entregue (veículo), quem entregará e quem receberá cada informação.

## 5.7 Consolidar Informações

De acordo com a IN-SLTI/MP 04/2014, a equipe de planejamento da contratação deve consolidar as informações geradas durante todo o processo de gestão de risco das contratações de TI e gerar o artefato "Análise de Riscos", o qual deverá conter [35]:

- Identificação dos riscos;

- Identificação das possibilidades de ocorrência e dos danos potenciais de cada risco identificado;
- Definição das ações a serem tomadas para reduzir ou eliminar as chances de ocorrência do evento;
- Definição das ações de contingência a serem tomadas caso o risco se concretize;
- Definição dos responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência.

Com todas as informações levantadas nos processos anteriores, a equipe de planejamento tem todo o artefato disponível no Apêndice B, pronto para aprovação necessária da autoridade competente.

### 5.7.1 Aprovar Gestão de Riscos

O gestor de TI deve avaliar todo o documento de Análise de Riscos para verificar se as informações atendem as necessidades da organização. Caso estejam de acordo, o gestor deve registrar, juntamente com a equipe de contratação, a aprovação da análise de riscos da respectiva contratação de TI e encerra-se, dessa forma, o processo de gestão de riscos das contratações de TI da FUNASA. Caso contrário, o gestor de TI deve notificar a equipe de contratação da necessidade de realizar novamente a reanálise e fornecer descrições das questões identificadas como necessárias a serem modificadas que foram incluídas ou excluídas da gestão de riscos. Após realizados os ajustes, devem ser realizadas novamente a análise do gestor, visando sua aprovação.

## 5.8 Fonte de Dados

O PMBOK (2013) descreve que uma metodologia deve definir fontes de dados que possam ser usados para realizar o gerenciamento dos riscos no projeto [67]. Como forma de auxiliar a equipe de contratação na elaboração da gestão de riscos das contratações de TI da FUNASA, foram reunidas em uma fonte de dados, um conjunto de riscos e controles já estabelecidos pelo "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" do TCU, que contempla uma base referencial para auxiliar a identificação de riscos e controles no planejamento da contratação de soluções de TI. Tal base de dados poderá compor a fase de identificação de riscos da presente proposta de metodologia nas contratações de TI da FUNASA, e a cada novo projeto, poderão ser complementadas com os novos riscos identificados, formando uma base de conhecimento que irá agregar boas práticas já utilizadas durante o planejamento das contratações de TI [24].

# Capítulo 6

# Considerações Finais

O sucesso nas contratações de soluções de TI é um dos principais objetivos dos gestores de TI na APF. As entidades, cada vez mais, dependem dos investimentos nesta área para que possam cumprir com suas missões institucionais e alcançar os objetivos estratégicos traçados e, para tanto, é necessário um bom planejamento da contratação, aderente às leis e normas e com a máxima eficiência frente aos recursos disponíveis.

A contratação de soluções de TI, assim como qualquer processo de aquisição, está sujeita aos riscos inerentes ao negócio. Uma efetiva contratação passa necessariamente pela antecipação e prevenção dos riscos a que o projeto pode ser exposto. Neste contexto, a gestão dos riscos é a ferramenta que auxilia os gestores para contratações mais seguras e efetivas.

O presente trabalho encontra escopo na proposição de uma metodologia de gestão de riscos aplicada às contratações das soluções de TI da Fundação Nacional de Saúde, que possibilite aos gestores, envolvidos no processo de contratação, tornar a disciplina de riscos nas contratações uma realidade dentro da entidade, adentrando em suas características e propriedades para que possam obter resultados práticos de sucesso nos projetos de compras de TI.

A gestão de riscos busca alinhar o gerenciamento de TI aos objetivos do negócio, balanceando custos e benefícios, garantindo a entrega dos serviços. A metodologia de gestão de riscos proposta buscou apresentar uma estrutura de processo de ponta a ponta para um gerenciamento de riscos bem-sucedido nas contratações de TI, orientando os envolvidos no processo, incluindo ferramentas e técnicas para compreender e gerir riscos concretos para os projetos de aquisição em TI no âmbito da FUNASA.

A aderência completa aos níveis de serviço ideais da solução aumenta as chances de êxito da compra de TI a ser realizada, considerando os riscos e impactos da contratação. A relação entre as etapas do modelo reforça a ideia de que cada passo é importante para a construção de uma gestão de riscos eficaz.

As fases que compõem a proposta (definição do contexto, identificação, análise e avaliação, tratamento, monitoramento e controle e consolidação das informações dos riscos) indicam, por intermédio das atividades e tarefas, as responsabilidades, requisitos, entradas, saídas e as informações que contribuirão para entender como garantir mais segurança nos investimentos, reduzindo ameaças e controlando vulnerabilidades, além de proporcionar uma visão mais precisa dos riscos atuais e dos futuros relacionados a outras contratações de TI.

Os documentos produzidos e propostos na prática, poderão ser modificados e evoluídos de acordo com a necessidade, sendo uma fonte de conhecimento que passará por constante atualização. Para outros órgãos ou processos, é necessário que o artefato seja adaptado à realidade, bastando para isso que sejam considerados os conceitos desejados, e que não mudem a essência da metodologia proposta. É importante ressaltar que este estudo proposto surge no sentido de agregar mais informações, dados e materiais de referência ao processo de contratação de TI da FUNASA, em especial ao processo de análise de riscos da IN-SLTI/MP 04/2014, uma vez que quanto mais tal norma for estudada e colaborada, mais as atividades serão detalhadas, permitindo a uniformização da linguagem para ajudar a comunicação e a compreensão dos envolvidos durante o processo de contratação de TI.

Por fim, vale ressaltar que os projetos de contratação de TI demandam esforço considerável de diversas unidades do órgão contratante, onde observa-se, por exemplo, a necessidade de elaboração de diversos documentos (estudos técnicos preliminares, termo de referência, estimativas de preço, análises jurídicas, editais entre outros), além do esforço necessário para a implantação da solução em si e, todo este processo envolve, geralmente, grandes quantidades de recursos financeiros que afetam o mercado brasileiro de TI.

O trabalho buscou demonstrar toda a complexidade envolvida no tema e suas dificuldades de aplicação prática, afirmação esta corroborada com as dificuldades internas que cada instituição pública enfrenta, como a falta de servidores e recursos financeiros. A modelagem proposta busca o amadurecimento do órgão com relação às contratações de TI, contribuindo para internalização de procedimentos previstos na legislação e de boas práticas, tornando o órgão menos dependente de pessoas e menos vulnerável a mudanças ambientais, contribuindo para que a FUNASA exerça seu papel perante a sociedade.

## 6.1 Resultados Obtidos

Para a construção da metodologia proposta foram coletados e apresentados dados referentes à contratação de bens e serviços de TI na APF brasileira. Também foram abordados temas desde a legislação do governo brasileiro, tais como decretos, leis, normativos e guias relacionados à contratação de serviços de TI, às disciplinas, *frameworks*, normas

como a ABNT NBR ISO 31000 e ABNT NBR ISO 31010, até modelos de gestão de riscos adotados pela academia em artigos e livros científicos.

A partir dos elementos apontados pela literatura e pela legislação sobre o tema, em conjunto com a observação empírica da atual realidade do órgão, foi possível a construção de uma fonte consolidada de conhecimento, especialmente elaborada para o tema das contratações de TI. As informações coletadas formaram uma estrutura para a construção da metodologia para a gestão de riscos para as contratações de TI da FUNASA.

O trabalho propôs uma abordagem sistêmica, apresentando conceitos, atividades, tarefas, documentos, pessoas e processos que integram a gestão de risco aplicada à realidade da FUNASA. Os gestores do órgão demonstraram que a metodologia apresenta viabilidade para uma implementação prática no processo de contratação de TI. Apesar de utilizada instituição específica para a construção do modelo, o trabalho possui um nível de abstração suficiente para servir como material de referência para outras instituições, obtendo, dessa forma, melhorias consideráveis em TI, contribuindo para a prática da gestão de riscos de outros órgãos.

A metodologia proposta por esse trabalho, num total de 20 tarefas agrupadas em 11 atividades e 6 processos, procurou embasar o processo de trabalho da contratação de TI do órgão, com um material aprofundado sobre o assunto, podendo ser utilizado como modelo para adesão também em outros processos da organização.

Os artefatos produzidos estão em conformidade com a principal norma que orienta as contratações de TI no Governo Federal, a IN-SLTI/MP 04/2014. Outra importante contribuição do trabalho é a reunião de riscos e controles já estabelecidos pelo TCU como boa fonte de dados para novos projetos. Tal banco de informações conta com 66 riscos comumente encontrados na APF, o que, por si só, com sua implementação, poderia auxiliar a diminuir os índices de contratações malsucedidas no governo. A primeira mudança de paradigma sugerida está relacionada à maneira como a gestão de riscos é tratada no âmbito da APF. Para tanto, é necessário que os gestores de TI e os responsáveis pelos órgãos percebam a importância do tema e deem o devido destaque à gestão de riscos nos processos de contratação.

## 6.2 Trabalhos Futuros

Os resultados desta pesquisa podem subsidiar trabalhos futuros que abordem temas relacionados à gestão de riscos nas contratações de TI como:

- Elaborar um modelo de avaliação que estabeleça indicadores de desempenho em um modelo de maturidade da metodologia de gestão de riscos proposta;

- Estabelecer requisitos para elaboração de uma ferramenta de software que automatize todo processo;
- Desenvolver uma base de conhecimento de riscos da contratação, com os controles e ações realizadas por projetos anteriores, registrando as lições aprendidas das contratações e compartilhando com outros órgãos da APF;
- Promover a cultura de controles internos baseados em riscos, utilizando a compilação da legislação, da jurisprudência e dos normativos do órgão que afetam as contratações de TI;
- Propor a criação de mecanismos de controle sobre o andamento das contratações de TI;
- Realizar estudos de caso para se levantarem as principais ameaças e vulnerabilidades ao processo de contratação de TI, auxiliando as equipes de planejamento de contratação na identificação e tratamento dos riscos mais recorrentes, reduzindo retrabalho das equipes.

Internamente para a FUNASA, os próximos passos para adoção da metodologia proposta passam por:

- Capacitar os servidores que trabalham com as contratações de soluções de TI e em gestão de contratos;
- Aprovar norma com a metodologia proposta, para internalizar o processo e torná-la parte da cultura da instituição;
- Estabelecer a segregação de funções nos processos de trabalho das contratações de TI e de gestão dos contratos.

Serão selecionados projetos que servirão como piloto para aplicação da metodologia proposta. Os resultados trarão dados para o aperfeiçoamento da metodologia e adequação necessária para melhoria contínua do processo.

# Referências


[1] Associação BRASILEIRA DE NORMAS TÉCNICAS – ABNT. Iso 38500: 2009. *Governança corporativa de tecnologia da informação*, 2009. 11, 30, 34

[2] A. Kanungo I. Trboljevac A. Deshprabhu Adler, B. e R. Levenson. Tools of risk management. 2003. 27

[3] Samer Alhawari, Louay Karadsheh, Amine Nehari Talet, e Ebrahim Mansour. Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, 32(1):50–65, 2012. 10

[4] SR Aris, Noor Habibah Arshad, e Azlinah Mohamed. Conceptual framework on risk management in it outsourcing projects. *management*, 36:37–38, 2008. 22

[5] ISACA Information Systems Audit e Control Association. Cobit 5 - modelo corporativo para governança e gestão de ti da organização. 2012. xi, xiv, 17, 21, 88, 90

[6] Alexandre Fernandes BARBOSA, Alvaro Ribeiro Botelho JUNQUEIRA, MM LAIA, e FI FARIA. Governança de tic e contratos no setor público. In *CATI-Congresso Anual de Tecnologia da Informação*, 2006. 14

[7] Laurence Bellagamba. 4 estimating risk adjusted cost or schedule using fuzzy logic. In *INCOSE International Symposium*, volume 9, pages 241–246. Wiley Online Library, 1999. 28

[8] Dan Benta, Ioan Marius Podean, e Cristian Mircean. On best practices for risk management in complex projects. *Informatica Economica*, 15(2):142, 2011. 26

[9] Edward WN Bernroider e Milen Ivanov. It project management control and the control objectives for it and related technology (cobit) framework. *International Journal of Project Management*, 29(3):325–336, 2011. 30

[10] Barry W Boehm. Software risk management: principles and practices. *IEEE software*, 8(1):32–41, 1991. 16

[11] Abdelkader Bouti e Daoud Ait Kadi. A state-of-the-art review of fmea/fmeca. *International Journal of reliability, quality and safety engineering*, 1(04):515–543, 1994. 27

[12] Anna Corinna Cagliano, Sabrina Grimaldi, e Carlo Rafele. Choosing project risk management techniques. a theoretical framework. *Journal of Risk Research*, 18(2):232–248, 2015. 28

[13] Thomas A Carbone e Donald D Tippett. Project risk management using the project risk fmea. *Engineering Management Journal*, 16(4):28–35, 2004. 9, 71

[14] Marco Aurelio Chaves Cepik e Diego Rafael Canabarro. Governança de ti: transformando a administração pública no brasil. 2010. 5

[15] Chris Chapman e Stephen Ward. Project risk management: processes, techniques and insights. 2003. xi, 9, 17, 18, 19, 27, 28

[16] Robert J Chapman. *Simple tools and techniques for enterprise risk management*. John Wiley & Sons, 2011. xiv, 44, 53, 58, 60, 61, 63, 71, 74, 77, 78, 82, 83, 87

[17] Eric K Clemons, Sashidhar P Reddi, e Michael C Row. The impact of information technology on the organization of economic activity: The "move to the middle" hypothesis. *Journal of management information systems*, 10(2):9–35, 1993. 9

[18] Dale F Cooper. *Project risk management guidelines: managing risk in large projects and complex procurements*. John Wiley & Sons, Inc., 2005. 8

[19] Cláudio Silva da Cruz, Rejane Maria da Costa Figuereido, e Edméia Leonor Pereira de Andrade. Processo de contratação de serviços de tecnologia da informação para organizações públicas. 2011. 4, 15, 31, 39, 40

[20] BRASIL. Comitê Gestor da Internet no Brasil-CGI. Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: Tic governo eletrônico 2015. *Internet.*, 2016. 1, 4

[21] Vaz Wesley Daud JR, Antonio. *A descomplicada contratação de TI na administração pública*. Tangente editora, 2016. xi, 1, 14, 31, 32, 34, 39

[22] Bilmar Angelis de Almeida Ferreira, Jane de Oliveira Rabelo de Almeida, Paulo Roberto Corrêa Leão, e Núbia Ponte Gonçalves Silva. Gestão de riscos em projetos: Uma análise comparativa da norma iso 31000 e o guia pmbok®, 2012. *Revista de Gestão e Projetos*, 4(3):46, 2013. 9, 26

[23] BRASIL. Tribunal de Contas da União TCU. Acórdão nº 786/2006 – plenário, 2006. *Internet. http://www.lexml.gov.br/urn/urn:lex:br:tribunal.contas.uniao;plenario:acordao:2006-05-24;786i*, Maio 2006. 2

[24] BRASIL. Tribunal de Contas da União TCU. Guia de boas práticas em contratação de ti. *Internet. http://tinyurl.com/yddpn3yy*, 2012. 5, 14, 15, 52, 92

[25] BRASIL. Tribunal de Contas da União TCU. Relatório de levantamento – tc 003.732/2014-2. *Internet. http://portal.tcu.gov.br/comunidades/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/*, Novembro 2014. xi, 31, 33, 34

[26] BRASIL. Tribunal de Contas da União TCU. Acórdão nº 2622/2015 – plenário, 2015. *Internet. http://tinyurl.com/y9wbnjhx*, Outubro 2015. 14

[27] BRASIL. Tribunal de Contas da União TCU. Gestão de riscos para o tcu. *Internet. http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/*, Maio 2017. xiv, 23

[28] BRASIL. Secretaria de Fiscalização de Tecnologia da Informação. Tribunal de Contas da União TCU. Nota tÉcnica 07/2014. organização do sistema de governança de tecnologia da informação (ti). *Internet. http://portal3.tcu.gov.br/portal/pls/portal/docs/2691836.PDF*, Junho 2014. 1, 4, 5, 30

[29] BRASIL. Secretaria de Fiscalização de Tecnologia da Informação. Tribunal de Contas da União TCU. Acórdão nº 916/2015 - auditoria na gestão de contratos de ti. *Internet. http://tinyurl.com/ycrwxxfp*, 2015. 1, 5

[30] C de Freitas e C Gomez. Análise de riscos tecnológicos na perspectiva das ciências sociais. *Ciências, Saúde—Manguinbos. Brazil*, pages 485–504, 1996. 8

[31] Antonio José Saraiva de Oliveira Júnior, Arnaldo Ribeiro Gomes, e Guilherme de Vasconcellos Machado. Metodologia de auditoria com foco em processo e risco. *Revista do TCU*, (132):28–37, 2015. 11

[32] BRASIL. Fundação Nacional de Saúde Funasa. Manual de procedimentos de solicitação e aquisição de bens e serviços de tecnologia da informação. *No. MNP-MI-007A-2016*, Janeiro 2016. xi, 49, 50, 51

[33] Georges Dionne. Risk management: history, definition, and critique. *Risk Management and Insurance Review*, 16(2):147–166, 2013. 9

[34] BRASIL. Ministério do Planejamento. Guia de orientação para o gerenciamento de riscos. *Internet. https://governoeletronico.gov.br/*, Março 2013. xi, xiv, 2, 6, 11, 12, 48, 62, 64, 71, 73, 78, 79, 90

[35] BRASIL. Ministério do Planejamento. Instrução normativa nº 04, de 11 de setembro de 2014. dispõe sobre o processo de contratação de serviços de tecnologia da informação pela administração pública federal direta, autárquica e fundacional. *Internet. https://governoeletronico.gov.br/biblioteca/arquivos/in-4-2014/download*, Setembro 2014. xiv, 4, 14, 15, 39, 40, 49, 54, 62, 72, 74, 76, 85, 91

[36] BRASIL. Ministério do Planejamento. Metodologia de gestão de riscos de segurança da informação e comunicações do sistema de administratação dos recursos de tecnologia da informações do poder executivo federal - mgrsisp v2.0. *Internet. https://https://www.governoeletronico.gov.br/documentos-e-arquivos/OE1-RM2-Julho.pdf/view*, Agosto 2016. xi, xiv, 12, 43, 55, 56, 58, 59, 61, 62, 70, 71, 72, 75, 76, 80, 82, 83, 91

[37] BRASIL. Ministério do Planejamento e Controladoria Geral da União. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do poder executivo federal. Maio 2016. 13

[38] Diana Leite Nunes dos Santos e João Souza Neto. Avaliação da percepção da conformidade de processos de contratação de soluções de tecnologia da informação com a instrução normativa no 4/2010 da slti. *Revista do Serviço Público*, 64(1):77–107, 2014. 5

[39] Patrick Dunleavy. *Digital era governance: IT corporations, the state, and e-government*. Oxford University Press, 2006. 30

[40] K Eidesen, SJM Sollid, e T Aven. Risk assessment in critical care medicine: a tool to assess patient safety. *Journal of Risk Research*, 12(3-4):281–294, 2009. 27

[41] Jan Emblemsvåg e Lars Endre Kjølstad. Strategic risk analysis-a field version. *Management decision*, 40(9):842–852, 2002. 27

[42] Richard Fairley. Risk management for software projects. *IEEE software*, 11(3):57–67, 1994. 16

[43] BRASIL. Senado Federal. Constituição da república federativa do brasil. 1988. 11, 34

[44] BRASIL. Funasa. Portal da funasa. *http://www.funasa.gov.br/site/conheca-a-funasa/competencia/*, Acessado em: 18/06/2017. xi, 45, 47, 48

[45] BRASIL. Funasa. Regimento interno da funasa. *Internet. http://www.funasa.gov.br/site/conheca-a-funasa/estatuto/*, Acessado em: 18/06/2017. 48

[46] Antonio Carlos Gil. Como elaborar projetos de pesquisa. *São Paulo*, 5:61, 2002. 42, 43

[47] Antonio Carlos Gil. Métodos e técnicas de pesquisa social. In *Métodos e técnicas de pesquisa social*. Atlas, 2010. 42

[48] Neal S Gray. Pram it or walk away. *AACE International Transactions*, page R5, 1998. 16

[49] W. Min Guofeng, W. e Z. Weiwei. Study on the existing problems and countermeasures of project risk management in china. *Energy Procedia*, 13, 2011. 10

[50] David Hillson. The risk breakdown structure (rbs) as an aid to effective risk management. In *5th European Project Management Conference. Cannes, France*, pages 1–11, 2002. 28

[51] Yong Hu, Jianfeng Du, Xiangzhou Zhang, Xiaoling Hao, EWT Ngai, Ming Fan, e Mei Liu. An integrative framework for intelligent software project risk planning. *Decision Support Systems*, 55(4):927–937, 2013. 16, 26

[52] M Gordon Hunter. *Handbook of Research on Information Management and the Global Landscape*, volume 7. IGI Global, 2008. 30

[53] IEC IEC. Iso 31010: 2009-11. *Risk management–Risk assessment techniques*, 2009. 10, 19, 20, 27, 28, 29, 67, 72, 73, 87

[54] ISO31000 ISO. 31000: 2009 risk management–principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*, 2009. xi, xiv, 8, 17, 20, 44, 53, 54, 57, 58, 61, 64, 65, 71, 72, 76, 81, 87, 88

[55] INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE ITGI. Governance of outsourcing. *Rolling Meadows: ITGI, 2005*, 2005. 14

[56] Trevor A Kletz. *HAZOP and HAZAN: identifying and assessing process industry hazards*. IChemE, 1999. 28

[57] Ralph L Kliem e Irwin S Ludin. *Reducing project risk*. Gower Publishing, Ltd., 1997. 16

[58] K Knight. Risk management: an integral component of corporate governance and good management. *ISO Bulletin*, 10, 2003. 26

[59] SCL Koh, SM Saad, Ammar Ahmed, Berman Kayis, e Sataporn Amornsawadwatana. A review of techniques for risk management in projects. *Benchmarking: An International Journal*, 14(1):22–36, 2007. 8, 28, 61

[60] Nada Korac-Kakabadse e Andrew Kakabadse. Is/it governance: need for an integrated model. *Corporate Governance: The international journal of business in society*, 1(4):9–11, 2001. 30

[61] Melinda Lyons, Maria Woloshynowych, Sally Adams, e Charles Vincent. Error reduction in medicine. *Final report to the Nuffield Trust UK*, 2005. 27

[62] Terry Lyons e Martin Skitmore. Project risk management in the queensland engineering construction industry: a survey. *International journal of project management*, 22(1):51–61, 2004. 27

[63] Sara Marcelino-Sádaba, Amaya Pérez-Ezcurdia, Angel M Echeverría Lazcano, e Pedro Villanueva. Project risk management methodology for small firms. *International Journal of Project Management*, 32(2):327–340, 2014. 16, 26

[64] Arben Mullai. *Risk management system-risk assessment frameworks and techniques*. DaGoB (Safe and Reliable Transport Chains of Dangerous Goods in the Baltic Sea Region) Project Office, Turku School of Economics, Turku, Finland, 2006. 27, 28

[65] Institute of Risk Management. The risk management standard. 2002. xi, xiv, 17, 18, 72, 75, 76, 77, 80, 87

[66] HJ Otway, H Otway, e M Peltu. Regulation and risk analysis. *Regulating Industrial Risks-Science, Hazards and Public Protection*, pages 1–19, 1985. 9

[67] A PMBoK. Guide to the project management body of knowledge. *Project Management Institute, Pennsylvania USA*, 2013. xi, xiv, 8, 9, 17, 21, 22, 26, 27, 28, 30, 43, 59, 62, 65, 67, 69, 72, 73, 77, 78, 79, 81, 82, 83, 85, 86, 87, 88, 89, 92

[68] Grant Purdy. Iso 31000: 2009—setting a new standard for risk management. *Risk analysis*, 30(6):881–886, 2010. 16

[69] Tzvi Raz e David Hillson. A comparative review of risk management standards. *Risk Management*, 7(4):53–66, 2005. 9, 26

[70] Tzvi Raz e E Michael. Use and benefits of tools for project risk management. *International journal of project management*, 19(1):9–17, 2001. 16

[71] Miroslav Rebernik e Barbara Bradač. Idea evaluation methods and techniques. *Institute for Entrepreneurship and Small Business Management, University of Maribor, Slovenia*, 2008. 27

[72] Ortwin Renn. Risk analysis: scope and limitations. 1985. 10

[73] Antonio Rodríguez, Francisco Ortega, e Ramiro Concepción. A method for the evaluation of risk in it projects. *Expert Systems with Applications*, 45:273–285, 2016. 26

[74] Carlos Alberto Corrêa Salles Júnior, Alonso Mazini SOLER, José Angelo S do VALLE, e Roque Junior RABECHINI. Gerenciamento de riscos em projetos. *Rio de Janeiro: Editora FGV*, 2006. 16

[75] Antonio Fernandes Soares Netto. *Proposta de artefato de identificação de riscos nas contratações de TI da Administração Pública Federal, sob a ótica da ABNT NBR ISO 31000: gestão de riscos*. 2013. 3, 4

[76] Álvaro Tamayo, Ana Magnólia Mendes, e Maria das Graças Torres Paz. Inventário de valores organizacionais. *Estudos de psicologia*, 5(2):289–315, 2000. 57

[77] Software Engineering Institute CMMI Product Team. Cmmi for acquisition, version 1.3. 2010. 89

[78] Hans Thamhain. Managing risks in complex projects. *Project Management Journal*, 44(2):20–35, 2013. 63, 65

[79] Paul C Tinnirello. *New directions in project management*. CRC Press, 2001. 9, 24

[80] Her Majesty Treasury. The orange book: Management of risk-principles and concepts. *London: HM Treasury*, 2004. xi, xii, xiv, 17, 19, 71, 78, 81, 82

[81] Federica Turra. La gestione del rischio nelle organizzazioni sanitarie italiane: analisi di aspetti culturali e metodologici secondo un approccio"human centred". 2008. 28

[82] Terry Williams. A classified bibliography of recent research relating to project risk management. *European Journal of Operational Research*, 85(1):18–38, 1995. 9

[83] Catherine Wright. Top three potential risks with outsourcing information systems. *Information Systems Control Journal*, 5:40–42, 2004. 14

[84] Robert K Yin. *Estudo de Caso-: Planejamento e Métodos*. Bookman editora, 2015. 43

# Apêndice A

# Lista de Verificação das Fontes de Riscos

**Data: __/__/__/**

**Participantes:**

| Fonte de risco | Descrição | Resposta | Observação |
|---|---|---|---|
| Áreas de negócio | A contratação está alinhada com PDTI? | | |
| | A contratação de TI está ligada a algum objetivo estratégico? | | |
| | A demanda foi solicitada informando modelo ou marca? | | |
| | Existe conhecimento do projeto na alta administração? | | |
| Processos | Existe processo devidamente formalizado para contratação de TI? | | |
| | A solução a ser contratada exige mudança de cultura da organização? | | |
| | Existe um levantamento da real necessidade de contratação de TI? | | |
| | Os requisitos técnicos da solução a ser contratada são bem definidas? | | |
| | Há uma justificativa para previsão de quantidade dos itens da solução de TI? | | |
| Recursos Humanos | A Equipe de planejamento tem perfil adequado para condução do processo de contratação de TI? | | |
| | Existe quantidade suficiente de pessoal para suportar a demanda de aquisições em TI? | | |
| | Existe comunicação e interação entre os membros da equipe de contratação? | | |
| | Os servidores indicados para equipe de planejamento dispõe de tempo para as atribuições de planejamento da contratação? | | |
| Recursos Financeiros | Existe orçamento designado para aquisição de TI? | | |
| | Existe sobra de produtos ou serviços, levando ao desperdício de recursos financeiros? | | |
| | Há uma análise de custo benefício da solução a ser contratada? | | |
| | Existe coleta concisa de cotação de preços? | | |
| | O preço da solução está dentro da média de mercado? | | |
| Legislação | Existe análise jurídica por área competente? | | |
| | A solução a ser contratada tem legislação própria que o controle? | | |
| | A especificação técnica atende à vários fornecedores? | | |
| | A solução de TI está parcelada? | | |
| Qualidade | Os requisitos técnicos são específicos de uma marca/modelo? | | |
| | Existe risco da solução atender apenas parcialmente o órgão? | | |
| | A solução é madura ou pode levar a descontinuidade antes do órgão desfrutar do investimento? | | |
| Tecnologia | A solução é de padrão proprietário? | | |
| | A solução é obsoleta ou está próxima de ser tornar obsoleta, o que levaria à descontinuidade antes do órgão desfrutar do investimento? | | |
| | Existe necessidade de contratação de outra solução de TI para que a solução a ser contratada funcione corretamente? | | |
| | Existe dificuldade para elaboração da especificação técnica? | | |
| Tempo | Pode ocorrer atraso no alcance dos resultados pretendidos com a contratação devido alguma intempestividade ou adequação do órgão? | | |
| | Pode ocorrer atraso no início dos trabalhos devido a contratada não possuir condições necessárias para a execução? | | |
| | Pode ocorrer atraso na finalização da contratação, paralisando algum serviço essencial do órgão? | | |

***Resposta**: (S) – SIM; (N) – Não; (N/A) – Não se aplica.*

# Apêndice B

# Proposta de Artefato de Análise de Riscos

| OBJETIVOS, ESCOPO, PREMISSAS E RESTRIÇÕES DO PROJETO | |
|---|---|
| **Objetivos do Projeto:** | Descrição dos Objetivos |
| **Nível de criticidade:** | (Baixa, Média, Alta) |
| **Escopo do Projeto:** | Descrição do Escopo |
| **Premissas do Projeto:** | Descrição das Premissas |
| **Restrições do Projeto:** | Descrição das Restrições |

| DEFINIÇÃO DAS PARTES INTERESSADAS ENVOLVIDAS | | | | | |
|---|---|---|---|---|---|
| Nome | Unidade | Telefone | Email | Papel | Responsabilidade |
| Nome1 | Unidade1 | Telefone1 | Email1 | Chefe1 | Responsabilidade1 |

| DEFINIÇÃO DO CICLO DE ACOMPANHAMENTO E REVISÃO | | |
|---|---|---|
| Data | Ação | Descrição |
| 10/10/2017 | Acompanhar | Validar informações sobre o primeiro ciclo de identificação dos riscos. |

| DEFINIÇÃO DAS CATEGORIAS DE RISCOS | | |
|---|---|---|
| Classificação | Categoria | Descrição |
| Interno | Financeiros | Incerteza em relação às fontes de financiamento e orçamento. |
| Externo | Políticos | Mudança de governo; mudança no cenário político; decisões sobre políticas interministeriais; mudanças na máquina do governo; terrorismo etc.; |

| FONTES DE RISCOS E ÁREAS DE IMPACTO | | | | | |
|---|---|---|---|---|---|
| ID | Fonte | Unidade | Responsável | Descrição | Data |
| 01 | Pessoas | Financeiro | Maria | Chefe da área financeira, responsável pela utilização da solução de TI a ser contratada. | 09/09/17 |
| 02 | Processos | Administrativo | José | Falta de processo estabelecido para verificação de reajustes financeiros da solução contratada. | 15/09/17 |

| RISCOS QUE COMPROMETEM O SUCESSO DA CONTRATAÇÃO | | | | | | |
|---|---|---|---|---|---|---|
| ID | Categoria | Fonte | Descrição do Risco | Impacto | Responsável | Data |
| 01 | Processos | 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Diretor executivo. | 09/09/17 |
| 02 | Políticos | 01 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Diretor administrativo. | 15/09/17 |

| RISCOS DE NÃO ATENDIMENTO DAS NECESSIDADES | | | | | | |
|---|---|---|---|---|---|---|
| ID | Categoria | Fonte | Descrição do Risco | Impacto | Responsável | Data |
| 01 | Tecnológico | 01 | Falta de requisito técnico de atendimento das necessidades. | Prestação parcial dos serviços. | Gestor de TI. | 09/09/17 |
| 02 | Financeiro | 01 | Falta de limite orçamentário. | Falta de produtos ou serviços. | Diretor administrativo. | 15/09/17 |

| IDENTIFICAR CONTROLES | | | | |
|---|---|---|---|---|
| **ID CONTROLE** | **ID RISCO** | DESCRIÇÃO | SITUAÇÃO / JUSTIFICATIVA | VULNERABILIDADE |
| Id1 | Id_risco1 | Descrição1 | Situação1 | Vulnerabilidade1 |

***Planejamento da contratação – Análise de Riscos***

*Análise e avaliação dos riscos*

| ID do Risco | **Descrição do Risco** | **Dano** |
|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Área requisitante do bem ou serviço de TI sem condição de prestar um serviço. |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais |

| ID do Risco | **Descrição do Risco** | **Impacto** | **Tipo do Impacto** | **Nível** |
|---|---|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Paralisação de serviços. | Alto |

| ID do Risco | Descrição do Risco | Ameaças | Nível do Impacto | Probabilidade | Nível de Risco |
|---|---|---|---|---|---|
| 01 | Atraso no processo de contratação. Causa: falta de pessoal especializado. | Paralisação de serviços essenciais. | Alto | Médio | **Alto risco** |
| 02 | Alteração de escopo do objeto da contratação. Causa: falta de definição objetiva das necessidades | Serviços sem continuidade, falta de produtos ou equipamentos e impossibilidade de alcance dos objetivos institucionais | Alto | Alto | **Alto risco** |



| ID do Risco | Descrição do Risco | Nível de Risco | Controles | Estimativa para implementação | | | Restrições | Opção para Tratamento | Ações de Prevenção | Responsável |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Custo | Prazo | Esforço | | | | |
| 01 | Coleta insuficiente de preços, levando a estimativas de preços sem o devido embasamento. | Alto risco | A equipe de planejamento deve consultar diversas fontes para obter preços a serem usados nas estimativas de preço da contratação de TI. | Custos relativos à telefone, internet e correio. | 3 meses | Nome1, Nome2, Nome3 | Sem restrições | Eliminar | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |
| | | | A equipe de contratação deve utilizar índices para ajustar os preços obtidos diretamente com os fornecedores. | Custos relativos à telefone, internet e correio. | 1 mês | Nome1, Nome2, Nome3 | Sem restrições | Mitigar | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |
| | | | Elaborar memória de cálculo das estimativas de preço, anexando evidências das pesquisas realizadas. | Custos com impressão | 3 meses | Nome1, Nome2, Nome3 | Sem restrições | Transferir | Ação1 | Resp1 |
| | | | | | | | | | Ação2 | Resp2 |
| | | | | | | | | | Ação3 | Resp3 |

***Planejamento da contratação – Análise de Riscos***

*Cronograma de tratamento dos riscos*

**Data: __/__/__/**

| Nível do Risco | ID | Risco | Prazo para Resposta | Observação |
|---|---|---|---|---|
| Alto risco | 01 | Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda às necessidades do órgão. | 30/05/2017 | |
| | 02 | Sobrecarga dos servidores responsáveis por atividades do processo de gestão de contratos. | 01/07/2017 | |
| | 03 | Falta de servidores na área de TI com domínio do processo de gestão contratual. | 30/07/2017 | |
| | 04 | Contratação com partes faltantes ou solução incompleta. | 01/08/2017 | |
| Risco moderado | 05 | Atraso do início dos trabalhos da contratada devido ao órgão não oferecer as condições necessárias para inícios dos trabalhos. | Finalização do processo de contratação | Monitorar até a conclusão. |
| | 06 | Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação de TI. | Finalização do processo de contratação | Monitorar até a conclusão. |
| | 07 | Coleta insuficiente de preços, levando a estimativa inadequadas. | Finalização do estudo técnico preliminar. | Monitorar até a conclusão. |
| | 08 | Utilização de somente uma solução do mercado como base para a definição de requisitos, levando ao direcionamento. | Finalização do estudo técnico preliminar. | Monitorar até a conclusão. |
| | 09 | Falta de passagem de conhecimento entre fornecedor e o órgão. | Finalização do contrato | Monitorar |

***Planejamento da contratação – Análise de Riscos***

*Monitorar e Controlar os Riscos*

**Data: __/__/__/**

| Nível do Risco | ID | Risco | Ações de Tratamento | Progresso de Implantação | Status Implementação | Prazo para Resposta | Observação |
|---|---|---|---|---|---|---|---|
| Alto risco | 01 | Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda às necessidades do órgão. | Ação1 | 100% | Implementado | 30/05/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 100% | Implementado | | |
| | 02 | Sobrecarga dos servidores responsáveis por atividades do processo de gestão de contratos. | Ação1 | 10% | Incompleto | 01/07/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 100% | Implementado | | |
| | 03 | Falta de servidores na área de TI com domínio do processo de gestão contratual. | Ação1 | 10% | Incompleto | 30/07/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 100% | Implementado | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 04 | Contratação com partes faltantes ou solução incompleta. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| Risco moderado | 05 | Atraso do início dos trabalhos da contratada devido ao órgão não oferecer as condições necessárias para inícios dos trabalhos. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 06 | Dificuldade dos atores envolvidos de justificar a adequação das | Ação1 | 10% | Incompleto | 01/08/2017 | |
| | | | Ação2 | 20% | Incompleto | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | estimativas de preço da contratação de TI. | Ação3 | 30% | Incompleto | | Descrição das ações realizadas. |
| | 07 | Coleta insuficiente de preços, levando a estimativa inadequadas. | Ação1 | 100% | Implementado | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 100% | Implementado | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 08 | Utilização de somente uma solução do mercado como base para a definição de requisitos, levando ao direcionamento. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |
| | 09 | Falta de passagem de conhecimento entre fornecedor e o órgão. | Ação1 | 10% | Incompleto | 01/08/2017 | Descrição das ações realizadas. |
| | | | Ação2 | 20% | Incompleto | | |
| | | | Ação3 | 30% | Incompleto | | |

| PLANO DE COMUNICAÇÃO DE RISCOS | | | | | | |
|---|---|---|---|---|---|---|
| **ID** | Evento | Informação | Periodicidade | Forma de Comunicação | Responsável | Parte Interessada |
| **01** | Incidente | Risco | Mensal | Email | Equipe de contratação | Área demandante da solução |

# Apêndice C

# Conjunto de Riscos e Controles para as Contratações de TI

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 01 | Contratação de uma solução de TI que não atenda à necessidade de negócio que a desencadeou, podendo causar impactos como: a) ocorrência de muitos ajustes; b) abandono da solução. | 1) publicar normativo estabelecendo a obrigação da área requisitante da solução de TI de participar ativamente de todo o processo de planejamento da contratação e da gestão do contrato, em especial da elaboração dos estudos técnicos preliminares. Convém que a responsabilidade por esse controle seja da alta administração; 2) publicar normativo estabelecendo a obrigação da alta administração ou de alguma estrutura de governança de TI de aprovar os artefatos das principais contratações de TI (e.g. as de maior importância ou materialidade), submetidos pela área de TI, de modo que a alta administração verifique a adequação da definição da necessidade de cada uma dessas contratações. Convém que a responsabilidade por esse controle seja da alta administração. |
| 02 | Descrição da necessidade da contratação em termos de TI e não de negócio, de modo que as justificativas sejam puramente técnicas, sem uma relação clara entre alguma necessidade do órgão e a contratação da solução. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 03 | Adoção de tipo de solução obsoleto ou próximo da obsolescência, levando à descontinuidade da solução antes do órgão conseguir desfrutar do investimento feito na solução. | 1) a equipe de planejamento da contratação deve verificar a perspectiva de amadurecimento de cada tipo de solução em análise, descartando aquelas consideradas obsoletas ou próximas da obsolescência, com as devidas justificativas explicitadas nos autos do processo de contratação. |
| 04 | Contratação de uma solução que poderia ter sido evitada ou ter sido executada em melhores condições (e.g. melhores definições de requisitos) se os processos de trabalho a serem suportados pela solução tivessem sido otimizados ou repensados antes da contratação. | 1) publicar normativo estabelecendo a obrigação da área requisitante da solução de TI de elaborar declaração, nos autos do processo, de que os esforços para otimizar os processos de trabalho existentes se esgotaram ou não são suficientes para que o órgão alcance os resultados pretendidos com a contratação. Convém que a responsabilidade por esse controle seja da alta administração; 2) publicar normativo estabelecendo a obrigação da alta administração ou de alguma estrutura de governança de TI de aprovar os artefatos das principais contratações de TI (e.g. as de maior importância ou materialidade), submetidos pela área de TI, de modo que a alta administração verifique se as melhorias dos processos de trabalho relativas a cada uma dessas contratações se esgotaram ou não são suficientes para que o órgão alcance os resultados pretendidos. Convém que a responsabilidade por esse controle seja da alta administração. |
| 05 | Manutenção de uma solução em atividade que não atenda mais a uma necessidade do órgão, seja porque a solução não consiga mais atender a essa necessidade, seja porque essa necessidade deixou de existir. | 1) a alta administração deve publicar normativo definindo qual é a unidade gestora de cada solução de TI do órgão, que normalmente é a área requisitante da solução, e quais são as obrigações dessa unidade com relação à solução de TI. Entre essas obrigações deve estar incluída a verificação da pertinência da solução de TI em termos de negócio a cada prorrogação do contrato ou repactuação, observando aspectos como economicidade, eficácia e eficiência. |
| 06 | Adoção de tipo de solução baseado em locação antieconômica de equipamentos ou softwares. | 1) a equipe de planejamento da contratação deve avaliar a economicidade desse tipo de contratação em comparação com a possibilidade de aquisição dos respectivos produtos, buscando o tipo de solução mais econômico. |
| 07 | Execução de contratações desalinhadas dos objetivos estabelecidos nos planos do órgão governante superior, do órgão e de TI do órgão, deixando-se de investir em iniciativas que contribuam para o alcance destes objetivos. | 1) a alta administração do órgão deve garantir a existência dos planos do órgão e de TI; 2) a alta administração deve aprovar o resultado do planejamento conjunto das contratações de soluções de TI e do orçamento de TI, a ser submetido pela área de TI, verificando o alinhamento das contratações previstas com os objetivos que constam dos planos do órgão governante superior ao qual o órgão está vinculado, do órgão e de TI do órgão, em especial as contratações de maior importância ou materialidade. Ressalta-se que o planejamento conjunto das contratações de soluções de TI e do orçamento de TI, idealmente, ocorre no âmbito do planejamento de TI do órgão, ou seja, seu resultado (plano de contratações de TI) deve fazer parte de planos como o PDTI; 3) publicar normativo estabelecendo a obrigação da alta administração ou de alguma estrutura de governança de TI de aprovar os artefatos das principais contratações de TI (e.g. as de maior importância ou materialidade), submetidos pela área de TI, de modo que a alta administração verifique se foi estabelecido o alinhamento entre cada uma dessas contratações e os planos do órgão governante superior ao qual o órgão está vinculado, do órgão e de TI do órgão. Convém que a responsabilidade por esse controle seja da alta administração. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 08 | Estabelecimento de requisitos desconectados da necessidade da contratação. | 1) publicar normativo estabelecendo a obrigação da revisão dos artefatos produzidos no planejamento das contratações por servidor sênior, de modo a verificar se somente foram definidos os requisitos mínimos para o atendimento à necessidade da contratação. Convém que a responsabilidade por esse controle seja da alta administração. |
| 09 | Estabelecimento de requisitos que limitem a competição e, por isso, contratar por preços elevados. | 1) a equipe de planejamento da contratação deve verificar se os requisitos estabelecidos são atendidos por quantidade expressiva de soluções de TI do nicho de mercado que supostamente atende à necessidade da contratação. Se o número for considerado restrito, verificar se os requisitos que limitam a participação são realmente indispensáveis, de modo a avaliar a retirada ou flexibilização destes requisitos. |
| 10 | Sobre preço em licitações baseadas no princípio da padronização (Lei 8.666/1993,art. 15, inciso I 153), mesmo quando há mais de um revendedor ou distribuidor do produto, devido a possível interferência do fabricante do produto. | 1) a equipe de planejamento da contratação deve levantar preços, não só do produto definido, como de outros do mercado que atendam aos requisitos, para elaborar juízo adequado de economicidade; 2) caso o preço final da licitação seja acima do preço máximo aceito, o órgão deve avaliar a possibilidade de abandonar a padronização, efetuando licitação sem restrição relativa à padronização. |
| 11 | Adoção de tipo de solução que siga predominantemente padrões proprietários, levando à dependência excessiva do órgão com relação à solução. | 1) a equipe de planejamento da contratação deve buscar contratar solução que siga padrões de mercado que permitam a migração para outras soluções (e.g. exigir que a solução ofereça facilidades de exportação dos dados em padrão que permita a importação desses dados por outras soluções). |
| 12 | Adoção de tipo de solução imaturo, levando a problemas na implantação ou descontinuidade da solução antes do órgão conseguir desfrutar do investimento feito na solução. | 1) a equipe de planejamento da contratação deve verificar se cada tipo de solução em análise conta com base instalada significativa, se muitos fornecedores do mercado oferecem soluções desse tipo e se apresenta perspectiva de amadurecimento, descartando aquelas consideradas imaturas, com as devidas justificativas explicitadas nos autos do processo de contratação. |
| 13 | Definição de requisitos e elementos contratuais que propiciem a ingerência do órgão sobre a administração da contratada, caracterizando execução indireta ilegal, contendo procedimentos, tais como : a) exigência dos funcionários da contratada trabalharem dentro das instalações do órgão sem justificativa; b) submissão dos funcionários da contratada à avaliação do órgão, tais como exames de admissão, entrevistas ou assemelhados; c) definição dos salários a serem pagos pela contratada aos seus funcionários; d) exigência de assinatura de Termo de Responsabilidade e Sigilo para acesso às informações e aos sistemas do órgão diretamente junto aos funcionários da contratada, devendo-se exigir que a contratada obtenha esse compromisso junto aos seus funcionários, bem como a fiscalização de seu fiel cumprimento; e) indicação de pessoa para ser contratada pelo fornecedor. | 1) a equipe de planejamento da contratação deve definir, no modelo de execução do objeto, que: a) os funcionários da contratada somente devam trabalhar dentro das instalações do órgão se for estritamente necessário, com a devida justificativa; b) a interação entre o órgão e a contratada ocorra essencialmente por intermédio do preposto, com exceção de serviços que exijam interação direta entre os usuários do serviço e a contratada (e.g.service desk); c) aspectos relativos à relação contratual entre a contratada e seus funcionários (e.g. solicitação de férias e avaliação de desempenho individual) sejam trata dos entre essas duas partes, sem interferência do órgão; d) no caso da adoção, excepcional, de modelo de execução indireta pela alocação por postos de trabalho, também conhecidas como contratação por body shopping, o órgão deva se restringir a fazer com que a contratada cumpra o modelo de execução do objeto citado, que deve definir claramente elementos que incluam: 1) a qualificação técnica necessária para assumir cada posto de serviço; e 2) os documentos que servirão para comprovar a qualificação exigida junto ao órgão; e) o Termo de Responsabilidade e Sigilo para acesso às informações e aos sistemas do órgão seja coletado pela contratada junto a cada funcionário seu e entregue ao órgão, de modo que não seja coletado diretamente pelo órgão junto aos funcionários a contratada; 2) publicar normativo vedando a indicação de pessoas para serem contratadas pelos fornecedores, bem como divulgá-lo junto aos servidores do órgão. Convém que a responsabilidade por esse controle seja da alta administração. |
| 14 | A solução contratada ser incompleta, de forma a não atender à necessidade da contratação. | 1) a equipe de planejamento da contratação deve garantir que o levantamento de mercado seja criterioso e, no caso de soluções complexas, verificar junto a outros órgãos e a fornecedores se a solução definida é devidamente abrangente para gerar os resultados pretendidos, de modo a atender à necessidade do órgão. |
| 15 | Utilização de somente uma solução do mercado como base para a definição de requisitos, levando ao direcionamento da licitação. | 1) a equipe de planejamento da contratação deve garantir que o levantamento de soluções do mercado seja feito junto ao maior número de fontes possível, efetuando levantamento de contratações similares feitas por outros órgãos, consulta a sítios na internet (e.g. portal do software público), visita a feiras, consulta a publicações especializadas (e.g. comparativos de soluções publicados em revistas especializadas) e pesquisa junto a fornecedores. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 16 | Sobra de produtos ou serviços, levando ao desperdício desses itens e de recursos financeiros. | 1) a equipe de planejamento da contratação deve definir método para estimar as quantidades necessárias. Se preciso, deve buscar métodos e técnicas para estimar as quantidades dos itens da solução em outros órgãos da APF; 2) a equipe de planejamento da contratação deve fazer levantamento exaustivo da necessidade, de modo a evitar a celebração de aditivos ou novas contratações; 3) a equipe de planejamento da contratação deve documentar a aplicação do método adotado para o cálculo das estimativas das quantidades dos itens a contratar nos autos do processo de contratação, explicitando como os cálculos foram feitos (memorial de cálculo); 4) o fiscal do contrato de uma determinada solução de TI deve armazenar dados da execução contratual, de modo que a equipe de planejamento da contratação que elaborar os artefatos da próxima licitação da mesma solução ou de solução similar conte com informações de contratos anteriores (e.g. séries históricas de contratos de serviços contínuos), o que pode facilitar a definição das quantidades e dos requisitos da nova contratação (e.g. quantidades de chamados por tipo e por unidade de tempo em contrato de service desk). |
| 17 | Falta de produtos ou serviços para atender à necessidade da contratação, levando a um ou mais dos impactos a seguir: a) celebração de aditivos contratuais, que poderiam ter sido evitados. b) novas contratações, por licitação ou não, se o erro de estimativa tiver sido grande, com todo o esforço administrativo decorrente; c) quebra da padronização dos produtos contratados, devido à celebração de aditivos; d) perda do efeito de escala, no caso de celebração de aditivos ou de realização de novas contratações, o que leva a custo final maior do que no caso de se efetuar uma única contratação com a soma das quantidades contratadas separadamente; e) utilização de orçamento superior à prevista, no caso de celebração de aditivos ou de realização de novas contratações, pois termina-se contratando mais itens do que o planejado. Essa utilização de orçamento não prevista pode levar ao cancelamento da contratação de outros itens previstos no planejamento conjunto das contratações de soluções de TI e do orçamento de TI. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 18 | Levantamento de mercado deficiente, levando a licitação deserta, ou seja, nenhuma proposta ser apresentada na licitação. | 1) os mesmos controles internos sugeridos para o risco 15. |
| 19 | Proximidade inadequada entre servidores da equipe de planejamento da contratação e empresa(s) do mercado, levando à quebra da imparcialidade da equipe, resultando no direcionamento da licitação. | 1) a equipe de planejamento da contratação deve interagir com os fornecedores de forma cautelosa. Uma boa prática é enviar correspondência oficial a cada potencial fornecedor identificado, contendo elementos essenciais da contratação (e.g. necessidade, requisitos, quantidades), para que ele possa informar se tem condições de entregar solução que atenda aos requisitos e qual é o preço estimado dessa solução. 2) caso sejam necessárias reuniões entre o órgão e empresas do mercado, bem como demonstrações de produtos ou serviços durante o levantamento de mercado, a equipe de planejamento da contratação deve fazer com que esses eventos ocorram com pelo menos dois servidores do órgão e sejam documentados nos autos do processo de contratação. 3) se for necessário conhecer as instalações de empresas que sejam potenciais fornecedoras da solução, o órgão deve justificar essa necessidade nos autos do processo de contratação e identificar quais são essas empresas e agendar visitas a cada uma delas, devidamente planejadas (e.g. elaborar lista de itens a verificar nas visitas), com o custo a cargo do órgão, e não das empresas. |
| 20 | Paralisação de solução de TI pouco tempo depois de sua instalação por falta de consumíveis (e.g. esgotamento rápido de cartuchos de impressoras a laser). | 1) a equipe de planejamento da contratação deve estabelecer que a solução de TI a ser contratada inclua todos os consumíveis necessários para que funcione por período pré-determinado, de maneira que o órgão tenha tempo para planejar, executar licitação e receber novos materiais de consumo. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 21 | Avaliação da viabilidade da contratação ser feita de forma subjetiva, por não se saber ao certo quais são os resultados pretendidos com a contratação. | 1) a equipe de planejamento da contratação deve estabelecer que a solução de TI a ser contratada inclua todos os consumíveis necessários para que funcione por período pré-determinado, de maneira que o órgão tenha tempo para planejar, executar licitação e receber novos materiais de consumo. |
| 22 | Coleta insuficiente de preços, levando a estimativas inadequadas. | 1) a equipe de planejamento da contratação deve consultar diversas fontes para obter preços a serem usados nos cálculos das estimativas dos preços unitários e do preço global; 2) a equipe de planejamento da contratação deve utilizar deflatores para ajustar os preços obtidos diretamente com os fornecedores, pois estimativas de preço obtidas junto a fornecedores, antes da licitação, normalmente incluem folgas; 3) a equipe de planejamento da contratação deve elaborar memória de cálculo das estimativas de preço, isto é, registrar os procedimentos adotados para se obter as estimativas a partir dos preços coletados, bem como anexar as evidências das pesquisas realizadas (e.g. cópias de pesquisas em portais na internet de órgãos e empresas, ofícios do órgão a empresas solicitando propostas de preço, propostas de preço das empresas); 4) publicar normativo estabelecendo procedimento consistente para elaboração de estimativas de preço, a fim de orientar as equipes de planejamento das contratações de TI do órgão, inclusive nos casos de contratações diretas e adesões a atas de registro de preço. Por exemplo, estabelecer parâmetros sobre o que fazer com os preços coletados (e.g. calcular a média ou considerar o menor valor coletado), estabelecer critério para descarte de preços (e.g. descartar preços muito acima dos demais, pois distorceriam cálculos como o da média), bem como período para considerar os preços (e.g. somente considerar preços estabelecidos nos últimos noventa dias). Convém que esse controle seja executado pela área administrativa; 5) publicar normativo estabelecendo a obrigação da revisão dos artefatos produzidos no planejamento das contratações por servidor sênior, de modo a verificar se os preços dos itens a contratar foram estimados preliminarmente e de forma adequada. Convém que a responsabilidade por esse controle seja da alta administração. |
| 23 | Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação quando questionados (e.g. por cidadãos, entidades de classe ou órgãos de controle). | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 24 | Contratação de partes faltantes de uma solução incompleta a preços elevados devido à necessidade de execução de contratação por inexigibilidade ou por licitação com definição de objeto de fornecedor específico, para garantir a compatibilidade com o resto da solução já contratado. | 1) a equipe de planejamento da contratação deve garantir que o levantamento de mercado seja criterioso e, no caso de soluções complexas, verificar junto a outros órgãos e a fornecedores se a solução definida é devidamente abrangente para gerar os resultados pretendidos, de modo a atender à necessidade do órgão. |
| 25 | Divisão de solução de TI que não seja técnica ou economicamente divisível, resultando em contratações por inexigibilidade ou em licitações com poucos fornecedores, levando à obtenção de valores mais altos, em comparação à compra conjunta da solução. | 1) a equipe de planejamento da contratação deve avaliar se a solução é divisível ou não, levando em conta o mercado que a fornece. |
| 26 | Definição de resultados não realistas, gerando frustração na área requisitante, na área de TI e em outros interessados. | 1) a equipe de planejamento da contratação deve avaliar a possibilidade de a contratação alcançar os resultados esperados definidos pela área requisitante. Se a equipe de planejamento considerar que os resultados não são realistas, deve negociar com a área requisitante para ajustar as expectativas, planejando, assim, uma contratação viável. Caso a negociação não se mostre eficaz, a equipe de planejamento deve levar o caso às instâncias superiores. A impossibilidade de produzir resultados realistas nos termos da área requisitante enseja a inviabilidade da contratação. |
| 27 | Contratação de duas ou mais soluções em um mesmo objeto contratual, o que descumpre a fundamentação legal citada no presente texto e vai contra a jurisprudência do TCU, levando ao seguinte: a) dependência excessiva da contratada que presta diversos serviços no mesmo contrato, de forma que, se a empresa deixar de existir (e.g. devido a | 1) a equipe de planejamento da contratação deve contratar soluções distintas separadamente, verificando, para cada solução, se é possível dividi-la. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| | desentendimento entre os sócios ou falência), o órgão fica sem o atendimento a diversas necessidades simultaneamente, o que é menos provável de acontecer se cada serviço for prestado por várias empresas diferentes; b) os modelos de execução do objeto e de gestão do contrato tendem a ser vagos e ineficazes. Por exemplo, as multas estabelecidas normalmente são genéricas, de modo que podem ter pouca eficácia; c) diminuição da competitividade na licitação, por não permitir que empresas especializadas em alguma das soluções participem da licitação, uma vez que não fornecem o conjunto completo de soluções. Adicionalmente, os requisitos de habilitação (e.g. atestados de capacidade técnica) tendem a permitir somente a habilitação de grandes empresas, pois empresas menores terão dificuldade de apresentar comprovação da prestação de serviços referentes a todas as soluções. | |
| 28 | Não alcance dos resultados pretendidos com a contratação. | 1) a equipe de planejamento da contratação deve elaborar os artefatos de planejamento da contratação expostos no presente guia, de modo a aumentar as chances de obter solução de TI que alcance os resultados pretendidos. |
| 29 | Falta de servidores na área de TI com domínio do processo de gestão contratual, levando a gestão de contrato deficiente. | 1) a alta administração e a área de TI devem tomar providências para garantir: a) a existência de quantidade adequada de servidores para executar o processo de gestão dos contratos; b) a qualificação dessas pessoas para executar esse processo de trabalho; 2) a área de TI pode promover a formação de comunidade de prática de planejamento das contratações e de gestão dos contratos de soluções de TI, de forma que os servidores envolvidos nessas atividades possam compartilhar informações e conhecimentos, bem como tirar dúvidas sobre esses temas. |
| 30 | Sobrecarga dos servidores responsáveis por atividades do processo de gestão dos contratos, levando à execução inadequada desse processo. | 1) a alta administração e a área de TI devem tomar providências para dar a relevância adequada ao processo de gestão dos contratos, de maneira que os servidores alocados às atividades desse processo, bem como as respectivas chefias, deem-lhes prioridade em termos de alocação de recursos. Por exemplo, no planejamento de TI (e.g. elaboração do PDTI), a área de TI deve explicitar os esforços necessários para gestão dos contratos, considerando que parte dos servidores da área será alocada em atividades desse processo, que são indelegáveis, ou seja, que não são passíveis de execução indireta. |
| 31 | A análise de risco ser otimista, desconsiderando riscos relevantes. | 1) publicar normativo estabelecendo a obrigação da revisão dos artefatos produzidos no planejamento das contratações por servidor sênior, de modo a verificar a consistência da análise de risco, considerando lições aprendidas em outras contratações. Convém que a responsabilidade por esse controle seja da alta administração. |
| 32 | Falta de participação da área requisitante da solução de TI, especialmente com relação à construção e à manutenção da solução (e.g. desenvolvimento de novos módulos e elaboração de novos relatórios de sistema de informação), levando à execução inadequada do objeto. | 1) a alta administração deve publicar normativo definindo qual é a unidade gestora de cada solução de TI do órgão, que normalmente é a área requisitante da solução, e quais são as obrigações dessa unidade com relação à solução de TI. Entre essas obrigações deve estar incluída a participação na: 1) elaboração das ordens de serviço para construção e para a manutenção da solução de TI; 2) avaliação dos serviços e artefatos entregues, sob a perspectiva de atendimento à necessidade de negócio, com base nas ordens de serviço; 2) a alta administração e a área de TI devem tomar providências para conscientizar os gestores das soluções de TI a respeito da importância da participação deles na construção, manutenção e operação das soluções de TI. |
| 33 | Atraso no alcance dos resultados pretendidos com a contratação devido à intempestividade da adequação do ambiente do órgão (e.g. uma nova solução pode demandar o aumento da velocidade da rede interna do | 1) a equipe de planejamento da contratação deve estabelecer cronograma para a adequação do ambiente do órgão no âmbito do planejamento da contratação, bem como os responsáveis por esses ajustes, dentro e fora da área de TI; 2) a equipe de planejamento da contratação, com o apoio dos gerentes máximos da área de TI e da área requisitante, deve contatar todos os atores responsáveis pelas mudanças no ambiente do órgão |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| | órgão e dos links de acesso à internet e essas mudanças ocorrerem somente após a implantação da solução). | necessárias para que a solução gere os benefícios esperados, deixando todos cientes dessas mudanças e garantindo que elas ocorram de forma tempestiva com relação à implantação da solução. Uma boa prática é registrar os compromissos dos atores responsáveis por essas mudanças, por exemplo, mediante atas de reunião, que devem ser incluídas nos autos do processo de contratação. |
| 34 | Atraso do início dos trabalhos da contratada devido à intempestividade do órgão em oferecer as condições necessárias para o início dos trabalhos. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 35 | Devido a atraso do órgão em oferecer as condições necessárias para a contratada iniciar seus trabalhos, ela pode pleitear algum tipo de indenização, pois já terá alocado recursos sem poder obter retorno. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 36 | Falta de abrangência da análise de viabilidade da contratação, de modo não considerar os aspectos necessários. | 1) publicar normativo estabelecendo a obrigação da equipe de planejamento de elaborar uma lista de verificação (checklist) para servir como base das justificativas expostas na conclusão da análise de viabilidade da contratação. Convém que a responsabilidade por esse controle seja da alta administração. |
| 37 | Ocorrência de ato antieconômico. | 1) a equipe de planejamento da contratação deve avaliar se os resultados pretendidos são compatíveis com os preços estimados da contratação (análise de custo-benefício). |
| 38 | Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda à necessidade do órgão. | 1) publicar normativo estabelecendo a obrigação da revisão dos artefatos produzidos no planejamento das contratações por servidor sênior, de modo a verificar a consistência da definição do objeto da contratação. Convém que a responsabilidade por esse controle seja da alta administração. |
| 39 | Dificuldade dos atores envolvidos de justificar a contratação quando questionados (e.g. por cidadãos, entidades de classe ou órgãos de controle). | 1) publicar normativo estabelecendo a obrigação da equipe de planejamento da contratação de publicar os estudos técnicos preliminares na internet. Convém que a responsabilidade por esse controle seja da alta administração; 2) no caso da impossibilidade de publicação dos estudos técnicos preliminares na internet, a equipe de planejamento da contratação deve expor os itens da fundamentação da contratação no termo de referência ou no projeto básico de forma expressa, de maneira que todos os interessados tenham acesso a essa fundamentação. |
| 40 | Elaboração de expectativa otimista de prazo necessário para se chegar à implantação da solução, gerando frustração na área requisitante e na área de TI, bem como prejuízo à credibilidade da área de TI. | 1) a equipe de planejamento da contratação deve considerar prazos realistas para que a licitação seja concluída e para que as ações necessárias para implantar a solução sejam efetivadas por todos os atores responsáveis, tais como: a) providências para adequação do ambiente do órgão para que a solução atenda à necessidade de negócio, incluindo ações de unidades do órgão necessárias para alocar recursos à contratada, como espaço físico e conhecimento a ser passado por servidores do órgão (e.g. detalhes de requisitos para dirimir dúvidas da contratada); b) ações pactuadas com a contratada para que a solução esteja funcional para gerar os resultados pretendidos (e.g. apoio para a implantação da solução em ambiente de produção) ou para que a contratada esteja apta a gerar resultados, no caso de serviços contínuos (e.g. tempo para a contratada contratar e alocar pessoal para executar os serviços); c) ações necessárias para avaliar e testar os produtos entregues para verificar se estão de acordo com os termos do contrato, tanto por parte da área requisitante como da área de TI; 2) a equipe de planejamento da contratação deve elaborar cronograma com base em prazos executados em contratações passadas, bem como nas lições aprendidas nessas contratações; 3) a equipe de planejamento da contratação deve verificar se os prazos são considerados aceitáveis pela área requisitante. Se não for negociar requisitos e prazos com essa área. Caso a negociação não se mostre eficaz, a equipe de planejamento deve levar o caso às instâncias superiores. A impossibilidade de atendimento à necessidade da contratação nos termos da área requisitante enseja a inviabilidade da contratação. |
| 41 | Concessão de perfis de acesso a sistemas de informação e a outros recursos a funcionários da contratada, levando à ocorrência de eventos nocivos ao órgão (e.g. vazamento de informações). | 1) publicar Política de Segurança da Informação (PSI), Política de Controle de Acesso (PCA) e Política de Classificação da Informação (PCI). Convém que a responsabilidade por esse controle seja da alta administração; 2) a equipe de planejamento da contratação deve estabelecer a obrigatoriedade de cumprimento da PSI, da PCA e da PCI pela contratada no termo de referência ou no projeto básico, que deve |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| | | constar do Termo de Responsabilidade a ser entregue por todos os funcionários da contratada envolvidos com a contratação. 3) a alta administração e a área de TI devem garanti r que a execução indireta de atividades que envolvam acesso livre a todas as informações do órgão em meio digital (e.g. gerência de rede e de administração de banco de dados) ocorra somente em casos excepcionais, devidamente justificados. |
| 42 | Dependência excessiva com relação à contratada, que passa a deter o conhecimento dos processos de trabalho e das tecnologias empregadas mais do que o próprio órgão. | 1) a equipe de planejamento da contratação deve elaborar os procedimentos relativos à transferência de conhecimentos, como reuniões mensais, oficinas e treinamentos, bem como os produtos esperados desses procedimentos (e.g. atas das reuniões realizadas entre o órgão e a contratada, a serem incluídas nos autos do processo de fiscalização), e incluí-los no modelo de execução do objeto. |
| 43 | Pagamentos indevidos por serviços parcialmente executados ou não executados. | 1) a equipe de planejamento da contratação deve estabelecer listas de verificação para os aceites provisório e definitivo na etapa de planejamento da contratação, de modo que o fiscal e a comissão de recebimento tenham um referencial claro para atuar na fase de gestão do contrato. |
| 44 | Pagamentos superfaturados, isto é, com valores acima dos previstos no contrato. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 45 | Expectativa equivocada da participação de atores no planejamento da contratação. | 1) a equipe de planejamento da contratação deve vislumbrar as etapas necessárias para que todos os produtos e serviços previstos na solução sejam entregues, de modo a especificar aspectos como a logística da implantação da solução, em especial no modelo de execução do objeto. Deve buscar auxílio junto a outras unidades quando necessário, ao invés de esperar que estas unidades atuem espontaneamente. Adicionalmente, devem-se vincular sanções a cada obrigação estabelecida. |
| 46 | Aproveitamento de edital ou adesão a uma ata de registro de preço de outra instituição mais madura que contenha modelos de execução do objeto e de gestão do contrato para os quais o órgão não está preparado. | 1) publicar normativo estabelecendo a obrigação da equipe de planejamento da contratação de, antes de aproveitar edital de outra instituição ou propor a adesão a uma ata de registro de preço, executar os seguintes procedimentos: a) planejar a contratação, pelo menos com a elaboração dos estudos técnicos preliminares, para que o órgão reflita sobre a necessidade da solução e sobre outros elementos, tais como as quantidades de itens necessárias para o órgão atender à sua necessidade de negócio; os riscos envolvidos no âmbito do órgão; as providências para adequação do ambiente do órgão em função do impacto esperado dos trabalhos da contratada durante a construção, implantação e operação da solução, bem como da solução após a sua implantação; b) com base nos elementos do planejamento da contratação do órgão, avaliar todas as condições estabelecidas no contrato e decidir: 1) se é possível cumpri-las; 2) se são suficientes para que o órgão atenda à sua necessidade. Do contrário, a equipe de planejamento da contratação deve alterá-las, no caso de aproveitamento de edital, ou não aderir à ata de registro de preço. Convém que a responsabilidade por esse controle seja da alta administração. |
| 47 | Aproveitamento de edital ou adesão a uma ata de registro de preço de outra instituição menos madura que contenha modelos de execução do objeto e de gestão do contrato considerados insuficientes ao órgão (e.g. conjunto de sanções limitado). | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 48 | Contratação direta (dispensa ou inexigibilidade) sem que haja modelos adequados de execução do objeto e de gestão do contrato. | 1) publicar normativo estabelecendo a obrigação da equipe de planejamento da contratação de elaborar os mesmos artefatos necessários para as contratações via licitação (estudos técnicos preliminares, plano de trabalho e termo de referência ou projeto básico) nas contratações diretas, inclusive de empresas públicas. Convém que a responsabilidade por esse controle seja da alta administração. |
| 49 | Falta de instrumentos formais para trazer o contrato à normalidade no caso de desconformidades na execução do objeto (e.g. qualidade dos produtos abaixo do definido no contrato, atraso nas entregas). | 1) a equipe de planejamento da contratação deve definir claramente os critérios de qualidade a serem verificados nos produtos e serviços entregues; 2) a equipe de planejamento da contratação deve prever os procedimentos de recusa dos produtos e serviços, caso não atendam aos critérios estabelecidos; 3) a equipe de planejamento da contratação deve especificar cuidadosamente as sanções e glosas passíveis de serem aplicadas à contratada. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 50 | Recusa dos servidores mais capacitados do órgão para exercerem a função de fiscal de contrato ou participarem de comissões de recebimento, por considerarem alto o risco de serem responsabilizados caso alguma irregularidade na gestão contratual seja identificada. | 1) a alta administração deve publicar normativo definindo qual é a unidade gestora de cada solução de TI do órgão, que normalmente é a área requisitante da solução, e quais são as obrigações dessa unidade com relação à solução de TI. Entre essas obrigações, deve estar incluída a homologação dos produtos entregues ao longo do contrato, a capacitação dos diversos atores envolvidos com o uso da solução e a priorização das mudanças da solução ao longo do tempo, o que colabora com o fiscal e com a comissão de recebimento na execução do contrato. |
| 51 | Contratação de solução de TI por licitação do tipo "técnica e preço" por valor superior aos de outras licitações similares feitas na modalidade pregão, em função da aparente segurança que o tipo de licitação "técnica e preço" traria no sentido de obter soluções de melhor qualidade, em comparação com licitações na modalidade "pregão". | 1) se a solução for constituída de bens e serviços comuns, a equipe de planejamento da contratação deve estabelecer a modalidade de licitação pregão, como regra eletrônico. |
| 52 | Conluio entre as licitantes em licitações presenciais. | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 53 | Pontuação desproporcional de critérios técnicos opcionais. | 1) nos casos excepcionais de utilização do tipo de licitação "técnica e preço", a equipe de planejamento da contratação deve tomar os seguintes cuidados: a) elaborar planilha contendo a contribuição percentual de cada critério técnico de pontuação com relação ao total de pontos da avaliação técnica, evidenciando a coerência entre a relevância de cada critério opcional com a respectiva pontuação; b) evitar a utilização de pesos diferentes para os fatores de pontuação técnica, utilizando peso um para todos os fatores. Por exemplo, em vez de definir peso cinco para o fator "qualidade" e peso dois para o fator "desempenho", as pontuações absolutas dos critérios do fator "qualidade" devem ser maiores do que as pontuações absolutas do critério "desempenho", refletindo a importância relativa dos critérios do fator "qualidade". Ou seja, devem-se prover mais pontos para cada critério do fator "qualidade" do que para os critérios do fator "desempenho". Assim, as pontuações de todos os critérios tornam-se comparáveis umas com as outras, sem a necessidade de multiplicá-las pelos pesos dos respectivos fatores. |
| 54 | Coleta insuficiente de preços, levando a estimativas de preços sem o devido embasamento, resultando na aceitação de preços acima da faixa de preços praticada no mercado, especialmente em processo de contratação direta ou de adesão a uma ata de registro de preço. | 1) a equipe de planejamento da contratação deve consultar diversas fontes para obter preços a serem usados nos cálculos das estimativas dos preços unitários e do preço global. Estimativas dos preços; 2) a equipe de planejamento da contratação deve utilizar deflatores para ajustar os preços obtidos diretamente com os fornecedores; 3) a equipe de planejamento da contratação deve estimar os preços unitários, bem como os valores máximo e mínimo (inexequível) de cada item; 4) a equipe de planejamento da contratação deve elaborar memória de cálculo das estimativas de preço, isto é, registrar os procedimentos adotados para se obter as estimativas a partir dos preços coletados, bem como anexar as evidências das pesquisas realizadas (e.g. cópias de pesquisas em portais na internet de órgãos e empresas, ofícios do órgão a empresas solicitando propostas de preço, propostas de preço das empresas); 5) publicar normativo estabelecendo procedimento consistente para elaboração de estimativas de preço, a fim de orientar as equipes de planejamento das contratações de TI do órgão, inclusive nos casos de contratações diretas e de adesões a atas de registro de preço. Por exemplo, estabelecer parâmetros sobre o que fazer com os preços coletados (e.g. calcular a média ou considerar o menor valor coletado), estabelecer critério para descarte de preços (e.g. descartar preços muito acima dos demais, pois distorceriam cálculos como o da média), bem como período para considerar os preços (e.g. somente considerar preços estabelecidos nos últimos noventa dias). Convém que esse controle seja executado pela área administrativa; 6) publicar normativo estabelecendo a obrigação da revisão dos artefatos produzidos no planejamento das contratações por servidor sênior, de modo a verificar se os preços dos itens a contratar foram estimados adequadamente. Convém que a responsabilidade por esse controle seja da alta administração. |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| 55 | Proposta da contratada deixar de ser a mais vantajosa após a celebração de aditivos contratuais para aumentar os quantitativos de alguns itens da solução, devido ao chamado "jogo de planilha". | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 56 | Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação quando questionados (e.g. por cidadãos, entidades de classe ou órgãos de controle). | 1) os mesmos controles internos sugeridos para o risco anterior. |
| 57 | Consumo de todo ou grande parte do orçamento de TI com contratações não planejadas, por intermédio de adesões a diversas atas de registro de preço no fim do ano, na condição de "carona". | 1) a alta administração e a área de TI devem garantir que o planejamento conjunto das contratações de soluções de TI e do orçamento de TI ocorra no primeiro quadrimestre do exercício anterior; 2) a alta administração e a área de TI devem garantir que grande parte das contratações se inicie no primeiro semestre do exercício corrente, para que no segundo semestre possam ser concluídas as licitações mais complicadas e implantadas diversas das soluções licitadas ao longo do ano. |
| 58 | Planejamento da contratação deficiente, levando à necessidade de ajustes no contrato durante sua execução (e.g. necessidade de estabelecimento de obrigação para a contratada entregar relatório mensal sobre a execução dos serviços). | 1) publicar normativo estabelecendo a obrigação da equipe de planejamento da contratação de elaborar os artefatos de planejamento da contratação expostos no presente guia, de modo a aumentar as chances de obter solução de TI que alcance os resultados pretendidos e diminua a probabilidade de haver necessidade de ajustes no contrato durante sua execução. Convém que a responsabilidade por esse controle seja da alta administração; 2) a alta administração do órgão e a área de TI devem garantir que haja servidores na área de TI em quantidade suficiente para elaborar os artefatos de planejamento de todas as contratações de TI do órgão ou supervisionar adequadamente a elaboração desses artefatos por terceiros (e.g. contratação da elaboração do termo de referência ou projeto básico); 3) estabelecer processo de capacitação contínua dos servidores participantes de equipes de planejamento de contratações de TI e de atividades de gestão contratual nos normativos e na jurisprudência envolvidos, pois além da complexidade desses conhecimentos, frequentemente há publicação de novos normativos e jurisprudência sobre o assunto. Convém que a responsabilidade por esse controle seja da alta administração. |
| 59 | Falta de passagem de conhecimento entre a equipe de planejamento da contratação e a de gestão do contrato, levando à ausência de execução de todo ou parte do que foi definido no planejamento da contratação na etapa de gestão do contrato, resultando no não atendimento à necessidade que deu origem à contratação. | 1) publicar normativo estabelecendo: a) a obrigação da interação (e.g. reuniões) entre as equipes de planejamento da contratação e de gestão do contrato antes da assinatura do contrato; b) a obrigação da equipe de gestão do contrato de participar da reunião de alinhamento de entendimentos e expectativas. Convém que a responsabilidade por esse controle seja da alta administração. |
| 60 | Interrupção da construção, implantação ou uso da solução de TI devido a mudanças de pessoas no comando da área requisitante. | 1) a alta administração do órgão deve garantir a existência dos planos do órgão e de TI; 2) a alta administração deve aprovar o resultado do planejamento conjunto das contratações de soluções de TI e do orçamento de TI, a ser submetido pela área de TI, verificando o alinhamento das contratações previstas com os objetivos que constam dos planos do órgão governante superior ao qual o órgão está vinculado, do órgão e de TI do órgão, em especial as contratações de maior importância ou materialidade. 3) publicar normativo estabelecendo a obrigação da área requisitante da solução de TI de elaborar declaração, nos autos do processo, de que os esforços para otimizar os processos de trabalho existentes se esgotaram ou não são suficientes para que o órgão alcance os resultados pretendidos com a contratação. Convém que a responsabilidade por esse controle seja da alta administração; 4) publicar normativo estabelecendo a obrigação da alta administração ou de alguma estrutura de governança de TI de aprovar os artefatos das principais contratações de TI, submetidos pela área de TI, de modo que a alta administração verifique se as melhorias dos processos de trabalho relativas a cada uma dessas contratações se esgotaram ou não são suficientes para que o órgão alcance os resultados pretendidos. Convém que a responsabilidade por esse controle seja da alta administração; 5) publicar normativo estabelecendo a obrigação da alta administração ou de alguma estrutura de governança de TI de aprovar os artefatos das principais contratações de TI, submetidos pela área de TI, de modo que a alta administração verifique se foi estabelecido o alinhamento entre cada uma dessas contratações e os planos |

| ID | Riscos Identificados | Controles Sugeridos |
|---|---|---|
| | | do órgão governante superior ao qual o órgão está vinculado, do órgão e de TI do órgão. Convém que a responsabilidade por esse controle seja da alta administração. |
| 61 | Interferência de servidor que seja membro da equipe de planejamento da contratação e também seja sócio ou tenha ligações financeiras com empresa do mercado da solução de TI a contratar, levando ao direcionamento da licitação em favor dessa empresa. | 1) a alta administração do órgão e a área de TI devem garantir que haja servidores na área de TI em quantidade suficiente para elaborar os artefatos de planejamento de todas as contratações de TI do órgão ou supervisionar adequadamente a elaboração desses artefatos por terceiros (e.g. contratação da elaboração do termo de referência ou do projeto básico); 2) a área administrativa deve colher declarações de todos os servidores que farão parte da equipe de planejamento da contratação antes de designá-los, informando que não são sócios e que não têm ligações financeiras com empresas do mercado da solução de TI a contratar. |
| 62 | Interferência de membro da equipe de planejamento da contratação que também seja funcionário de empresa do mercado da solução de TI a contratar, levando ao direcionamento da licitação em favor dessa empresa. | 1) a alta administração do órgão e a área de TI devem garantir que haja servidores na área de TI em quantidade suficiente para elaborar os artefatos de planejamento de todas as contratações de TI do órgão ou supervisionar adequadamente a elaboração desses artefatos por terceiros (e.g. contratação da elaboração do termo de referência ou do projeto básico); 2) publicar normativo estabelecendo a vedação da participação de funcionários de empresas contratadas no planejamento das contratações de soluções de TI do órgão, com exceção da execução de atividades operacionais, tais como levantamentos para definir a quantidade de itens a contratar. Convém que a responsabilidade por esse controle seja da alta administração. |
| 63 | Elaboração dos artefatos de planejamento da contratação por empresa do mercado da solução de TI a contratar, levando ao direcionamento da licitação em favor dessa empresa. | 1) a alta administração do órgão e a área de TI devem garantir que haja servidores na área de TI em quantidade suficiente para elaborar os artefatos de planejamento de todas as contratações de TI do órgão ou supervisionar adequadamente a elaboração desses artefatos por terceiros (e.g. contratação da elaboração do termo de referência ou do projeto básico). |
| 64 | Estabelecimento de prazo curto demais para a apresentação de proposta relativa a uma solução de TI complexa em licitação do tipo pregão, de modo a favorecer fornecedor(es) específico(s) que tenham condições de oferecer propostas de forma mais rápida. | 1) em função da complexidade da solução, a equipe de planejamento da contratação deve encaminhar à equipe responsável pela condução da licitação (e.g. Comissão Permanente de Licitação) o prazo adequado para que as licitantes formulem propostas na etapa de seleção do fornecedor. Salienta-se que o prazo citado não pode ser inferior a oito dias úteis (Lei 10.520/2002, art. 4º, inciso V 158), mas esse prazo pode ser curto demais para se elaborar propostas para determinadas soluções de TI. |
| 65 | Condução de contratação efetuada pelo Sistema de Registro de Preços (SRP) sem o devido embasamento legal, em especial com relação ao enquadramento da contratação em uma das hipóteses contidas no art. 2º do Decreto 3.931/2001 159. | 1) publicar normativo estabelecendo a necessidade de embasar as contratações efetuadas pelo SRP. |
| 66 | Adesão a uma ata de registro de preços que apresente características ou condições contratuais específicas do órgão (ou conjunto de órgãos) que efetuou a contratação e que não valem para outros órgãos que efetuem adesões na condição de "carona", de modo que essas características tornem a adesão ilegal ou parcialmente ineficaz. | 1) publicar normativo estabelecendo a necessidade de verificar, antes de aderir a ata de registro de preço na condição de "carona", se na ata há características ou condições contratuais específicas do órgão (ou conjunto de órgãos) que efetuou a contratação. |