**UNIVERSIDADE DE BRASÍLIA**

**FACULDADE DE TECNOLOGIA**

**DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

# 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

**ANTONIO FERNANDES SOARES NETTO**

**ORIENTADOR: RAFAEL TIMÓTEO DE SOUSA JÚNIOR**

**CO-ORIENTADOR: EDGARD COSTA OLIVEIRA**

**DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA**

**PUBLICAÇÃO: PPGEE.DM – 521/2013**

**BRASÍLIA/DF: MARÇO – 2013**

**UNIVERSIDADE DE BRASÍLIA**

**FACULDADE DE TECNOLOGIA**

**DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

# 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

**ANTONIO FERNANDES SOARES NETTO**

**DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISÍTOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM ENGENHARIA ELÉTRICA.**

**APROVADA POR:**

**Prof. Rafael Timóteo de Sousa Júnior, Dr. (ENE-UnB)**

**(Orientador)**

**_____**

**Prof. Flávio Elias Gomes de Deus, Dr. (ENE-UnB)**

**(Examinador Interno)**

**_____**

**Cristiano da Rocha Heckert, Dr. (USP-SP)**

**(Examinador Externo)**

**BRASÍLIA/DF, 06 DE MARÇO DE 2013.**

**FICHA CATALOGRÁFICA**


NETTO, ANTONIO FERNANDES SOARES
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 [Distrito Federal] 2013.
xiii, 133p., 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2013). Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Governança de Tecnologia da Informação (TI) 2. Identificação de Riscos
3. Contratações de TI 4. Administração Pública Federal
I. ENE/FT/UnB II. Título (série)


**REFERÊNCIA BIBLIOGRÁFICA**


NETTO, A. F. S. (2013). 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. Dissertação de Mestrado em Engenharia Elétrica, Publicação 521/2013, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 133p.


**CESSÃO DE DIREITOS**

AUTOR: Antonio Fernandes Soares Netto.

TÍTULO: 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.

GRAU: Mestre ANO: 2013



_____


**Antonio Fernandes Soares Netto**

Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica
CEP: 70910-900 Brasília – DF. BRASIL

## DEDICATÓRIA

Ao meu grande Deus, que testou meus limites e me mostrou quem realmente sou.

À minha Mãe, Fátima Suely, por sua coragem e dedicação incondicional aos seus filhos.

À minha esposa, Krisley Amorim. Por me apoiar nas madrugadas de dedicação.

Aos meus irmãos, Douglas Soares e Caio Dantas, pela compreensão de minha ausência.

Ao meu pai Miguel Antonio Soares (*in memoriam*). É emocionante registrar aqui o quanto sua falta é difícil.

À minha linda, encantadora e amada filha: Melissa de Amorim Fernandes Soares, que um dia enfrentará com muita coragem os caminhos em busca do conhecimento.

Ao Bob. A lealdade de um cão supera a de alguns homens.

## AGRADECIMENTOS

Primeiramente aos professores e orientadores: Dr. Rafael Timóteo de Sousa Júnior, Dr. Edgard Costa Oliveira, Dr. Flávio Elias Gomes de Deus, Dr. Ricardo Staciarini Puttini, por toda paciência, disponibilidade e orientação.

Aos amigos: Dr. Cristiano Heckert (Conselho Nacional do Ministério Público), pelas ideias que inspiraram a concretização deste trabalho e Silvio Lima (Ministério do Planejamento), pelos direcionadores e apoio incondicional. Aos dois, pelos motivadores jogos de tênis.

Ao meu diretor, Maurício Marques, meu coordenador Ramon Barreto e ao amigo Clóvis Dorbestein, Presidência da República - Diretoria de Tecnologia, pelo apoio nesse projeto.

Aos amigos de GSISP da Presidência da República: Jorge Júnior por sua dedicação e parceria no projeto que coordenamos e Msc. Paulo Ângelo, pela confiança e otimismo.

A equipe de professores e alunos da ENAP/DGTI. Em especial à amiga Danielle Barreto.

Ao Msc. Cláudio Cruz - Tribunal de Contas da União e Dr. João Sousa Neto (Correios), motivadores e apoiadores dessa pesquisa logo em seu início.

Ao Diretor-Geral da ESAF, Msc. Alexandre Ribeiro Motta, por ter me recebido com cordialidade em sua concorrida agenda para troca de experiências sobre contratações.

Aos meus amigos Msc. Beatriz Santana, Msc. Eliane Carneiro, Msc. Tomás Orlandi e Msc. Paulo Freire, da UnB, que me apoiaram no pré-projeto desta pesquisa.

Ao meu treinador Luís Orione e às memórias de Ayrton Senna *(in memorian)*. Pelos aprendizados no esporte que refletiram em minha vida a busca incansável pela vitória.

Ao Rogério Olegário (Consultor), por guiar minhas deci$õe$ e escolhas mais importantes para meu futuro. À Ana Freiras *(Coach)* pelo trabalho desenvolvido em minha carreira.

À Carla, Adriana (ENE/UNB) e Marineide (Presidência da República), pelos bastidores.

À Universidade de Brasília, pelo incentivo por mérito aos seus servidores.

Muito obrigado às pessoas que, com uma palavra ou atitude positiva, desejaram sucesso nesta caminhada de pesquisa, superação, perseverança, paciência e autoconhecimento.

# EPÍGRAFE

"*Muitas das ideias que utilizei neste trabalho não são minhas. Elas são das normas, autores, modelos e órgãos pesquisados que abordam completa ou parcialmente o tema de riscos e contratações de TI: ABNT NBR ISO 31000, 31010, GUIA 73, Cruz (2008), Motta (2010), COBIT, PMBOK, Ministério do Planejamento (SLTI), Tribunal de Contas da União, dentre outros. Se você não gostar das ideias deles, quais são as que você usaria?"*

# RESUMO

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

**Autor: Antonio Fernandes Soares Netto**
**Orientador: Rafael Timóteo de Sousa Júnior**
**Co-orientador: Edgard Costa Oliveira**
**Programa de Pós-graduação em Engenharia Elétrica**
**Brasília, Março de 2013**

**Resumo**

Este trabalho teve como objetivo propor um artefato para Identificação de Riscos nas contratações de Tecnologia da Informação (TI) na Administração Pública Federal Brasileira (APF). Foram utilizados procedimentos metodológicos qualitativos e exploratórios de normas de riscos, originados da NBR ISO ABNT 31000 e *frameworks* de governança (COBIT e PMBOK), além de autores que abordam o tema, para construção de mapas mentais que permitiram a extração de categorias de informação. Estas categorias foram utilizadas para construção do artefato de Identificação de Riscos. Para validação do artefato foi realizado um estudo de caso, do qual permitiu-se inferir que, antes de sua existência, os gestores tinham como diretriz um artefato sem padronização metodológica para identificação de riscos. Com o uso do artefato, os gestores podem encontrar vulnerabilidades que antes não eram possíveis de ser observadas, o que permitirá uma melhoria na definição dos níveis de serviço e na gestão contratual, por meio de uma construção mais eficaz do termo de referência. Os resultados demonstram que o artefato servirá como uma fonte consolidada de informação para Identificação de Riscos nas contratações de TI na APF.

**Palavras chave**: Governança de Tecnologia da Informação (TI); Contratações de TI; Identificação de Riscos; Administração Pública Federal.

# ABSTRACT

PROPOSAL OF A RISK IDENTIFICATION ARTIFACT FOR IT PROCUREMENT WITHIN THE BRAZILIAN FEDERAL PUBLIC ADMINISTRATION FROM THE PERSPECTIVE OF ABNT NBR ISO 31000 - RISK MANAGEMENT.

**Author: Antonio Fernandes Soares Netto**
**Supervisor: Rafael Timóteo de Sousa Júnior**
**Co-Supervisor: Edgard Costa Oliveira**
**Programa de Pós-graduação em Engenharia Elétrica**
**Brasília, March of 2013**

**Resume**

This work is aimed at proposing an artifact for Risk Identification to be used within the Information Technology (IT) procurement process by the Brazilian Federal Public Administration (APF). A qualitative exploratory methodological approach was used to building mental maps representing information categories expressed in risks management standards, such as ABNT NBR ISO 31000, as well as best practices and governance frameworks (COBIT and PMBOK), and authors who have studied this subject. These categories were used to construct the proposed Risk Identification artifact. For the validation of this artifact, a case study was performed, which indicated that in the past situation when such an artifact was not available for managers, the risk identification in IT procurement was conducted in ad hoc processes and that, having the proposed artifact at hand a referential for risk identification could be established resulting in managers find vulnerabilities that were not previously possible to be observed, this way allowing to improve the service levels negotiations and contract management procedures, due to a more effective construction of the terms of reference. The results demonstrate that the proposed artifact constitutes a consolidated source of information for Risk Identification in Information Technology procurement processes by the Brazilian APF.

**Key words:** IT Governance; IT Procurement; Risk Identification; Federal Public Administration.

# SUMÁRIO

# LISTA DE FIGURAS

# LISTA DE TABELAS

# LISTA DE ACRÔNIMOS

| | |
|---|---|
| ABNT | Associação Brasileira de Normas Técnicas |
| APF | Administração Pública Federal |
| BPMN | *Bussiness Process Modeling Notation* |
| CF | Constituição Federal |
| CGU | Controladoria-Geral da União |
| COBIT | *Control Objectives for Information and related* |
| DGTI | Desenvolvimento de Gestores de Tecnologia da Informação |
| EGTI | Estratégia Geral de Tecnologia da Informação |
| ENAP | Escola Nacional de Administração Pública |
| GSISP | Gratificação Temporária do SISP |
| GR | Gestão De Riscos |
| IEEE | *Institute of Electrical and Electronics Engineers* |
| IN04 | Instrução Normativa 04 |
| ISO | *International Organization for Standardization* |
| ITGI | *IT Governance Institute* |
| MP | Ministério do Planejamento |
| OLA | *Organisational Level Agreement* |
| PDTI | Plano Diretor de Tecnologia da Informação |
| PMBOK | *Project Management Book of Knowledge* |
| PMI | *Project Management Institute* |
| QRN | Quadro Referencial Normativo |
| SEFTI/TCU | Secretaria de Fiscalização de TI / TCU |
| SISP | Sistema de Administração dos Recursos de Informação e Informática |
| SLA | *Service Level Agreement* |
| SLTI | Secretaria de Logística e Tecnologia da Informação |
| TCU | Tribunal de Contas da União |
| TI | Tecnologia da Informação |

# 1. INTRODUÇÃO

A melhoria contínua de processos organizacionais, que se constitui como um dos princípios da visão contemporânea da qualidade, vem sendo apontada por diversos autores como uma importante componente da racionalização dos gastos públicos no Brasil (MOTTA, 2010; GASPAR, 2005; FILGUEIRAS, 2009). Dentre tais gastos públicos, vale notar que uma parcela significativa corresponde às contratações de bens e serviços de Tecnologias da Informação (TI) que são de alta relevância orçamentária.

Nesse contexto, aprimorar o planejamento das contratações, alinhando-o com uma adequada identificação de riscos poderá evitar desperdícios dos serviços e produtos contratados. Somente no ano de 2010, o orçamento governamental para TI ultrapassou os R$ 12 bilhões de reais, segundo o Acórdão 2.308/2010 do Tribunal de Contas da União (TCU), incluindo contratações de órgãos com altos orçamentos no âmbito do executivo federal, que juntos compraram mais de 7000 soluções de TI somente em 2010 (CEPIK; CANABARRO, 2010). Tais montantes demonstram que é necessário observar as contratações de TI com atenção, pois podem estar cercadas de riscos, muitos deles ocultos por não terem sido identificados.

Mas para se comprar TI na estrutura da APF, geralmente é necessário que se realize um procedimento administrativo denominado "licitação", preconizado pela lei 8.666/93 que é lei de licitações (BRASIL, 1993). Há também um detalhamento das rotinas de contratação de TI da APF, especificado na Instrução Normativa SLTI/MP 04 (IN04) [1], norteadora para aquisição de tecnologia no governo.

Essa instrução normativa foi criada em 2008, como proposta de evolução da gestão das contratações públicas de TI, devido à verificação pelo Tribunal de Contras da União (TCU) de irregularidades em diversas contratações, entre os anos de 2003 e 2008. Motivado por esse fato, o TCU emitiu diversos acórdãos, dentre eles o acórdão 786/2006 TCU Plenário,

[1] Será considerada para o trabalho a IN04/2010, devido ao fato desta versão promover, por meio do Guia Prático para Contratação de Soluções de TI da APF, as rotinas e tarefas a serem executadas para se proceder com as contratações de TI. Portanto, onde se lê IN04, entenda-se IN04/2010. Não existe limitação em se utilizar a IN04/2012, entretanto como o desenho das atividades foi realizado entre 2010 e 2011 no Guia Prático para Contratação de Soluções de TI, optou-se por referenciar a versão de 2010. A versão de 2012 não apresentou mudanças que impactem na aplicação do trabalho.

item 9.2, o qual se refere à determinação para que SLTI/MP elaborasse um modelo de licitação e contratação de serviços de informática para a APF bem como promovesse a implantação deste modelo nos diversos órgãos e entidades do SISP - Sistema de Administração dos Recursos de Informação e Informática (CEPIK, CANABARRO, 2010; TCU, 2006).

Assim, em 2008 publicou-se a IN04. Dois anos depois, em 2010 foi proposta a primeira versão do Guia Prático para Contratação de Soluções de TI da APF, que apresentou um esclarecimento maior do processo, com exemplos e *templates* e descrição de atividades apresentados pela IN04. A IN04 foi atualizada nos anos de 2010 e 2012.

Em sua essência, o Guia Prático organiza papeis, responsabilidades e atividades que devem ser desempenhadas para uma contratação de TI, além de uma proposta de divisão de fases nas etapas de contratação. Apresenta também relação de documentos que servirão de apoio para a contratação e para sua gestão e, por fim, artefatos e modelos que irão compor o documento Termo de Referência (TR), com um conteúdo mínimo a ser especificado, na busca de maior segurança para a contratação.

O TR consolida o estudo prévio da contratação e geralmente é especificado por um dos papéis definidos na IN04, que é, segundo o art. 2, a área de Tecnologia da Informação dos órgãos públicos. Para conclusão desse estudo prévio que gera o TR, os gestores de TI devem confeccionar na fase de planejamento da contratação, os seguintes artefatos: Documento de Oficialização da Demanda, Plano de Sustentação, Análise de Viabilidade, Estratégia da Contratação e Análise de Riscos. Todo esse trabalho irá impactar nas demais fases do processo (ver Figura 2-9 e 2-10).

Uma questão comum entre integrantes da área de TI que atuam na confecção do TR é a discussão sobre a identificação dos riscos da contratação de TI. As preocupações variam de riscos técnicos, jurídicos, externos ou internos à organização, até se há realmente aderência ao negócio. Em muitos casos, os gestores se preocupam inclusive se o processo licitatório será concluído, pois uma contratação pode ter impactos nas fases seguintes, muitas vezes não previstos.

Para diminuir os riscos, os integrantes da equipe levantam a maior quantidade de riscos possíveis, utilizando o artefato Análise de Riscos proposto pela IN04. Entretanto esse documento é um *template* em branco que não contém um apoio metodológico ou

procedimental das rotinas de identificação de riscos. Não existe rastreabilidade nem monitoramento até a entrega da solução de TI, o que demonstra que faltam aportes teóricos e práticos para tal questão. Isso pode gerar indicadores equivocados para medição na fase de gestão contratual, o que consequentemente irá refletir em novas contratações, corretivas ou adicionais, utilizando então mais recursos públicos simplesmente por que os riscos necessários não foram previstos da maneira correta por falta de metodologia de identificação de riscos.

Para diminuir essa lacuna, foi considerada a Gestão de Riscos (GR), baseada em normas como a ABNT NBR ISO 31000, 31010 e GUIA 73. Neste contexto, risco é um tema de relevância e que tem sido muito utilizado nos últimos anos por organizações de todo o mundo em diversos segmentos devido sua aplicação multidisciplinar. Essa aplicação será então destinada ao contexto das contratações de TI com este trabalho.

Assim foi idealizada a utilização de um artefato para Identificação de Riscos nas contratações de TI na APF, sob a ótica das normas de riscos. Um artefato poderá permitir aos gestores de TI considerarem uma maior quantidade e qualidade de critérios de identificação de riscos para a contratação em questão.

Logo ficou definido o eixo desta pesquisa como **“Conjunto de Atividades e Artefatos para a melhoria da Identificação de Riscos nas Contratações de TI na APF, sob a Ótica de Normas de Riscos ISO/ABNT”.** Este eixo de pesquisa permitiu a definição do tema desta dissertação.

## 1.1 PROBLEMA

Entidades públicas especificam contratações de Tecnologia da Informação (TI) demandadas por áreas de negócio, com uma proposta de TR direcionado a área de licitações para compra do bem ou serviço necessário. Essas entidades públicas possuem políticas pré-estabelecidas pelo governo que está no poder. Para realizar contratações que irão apoiar tais políticas, existe um roteiro consolidado pelos órgãos para construção do TR que deve ser seguido. Esse roteiro inclui o planejamento da contratação seguido da fase de seleção do fornecedor e do gerenciamento do contrato, conforme preconiza a IN04 e o Guia Prático para Contratação de Soluções de TI.

O Guia possui o processo de Análise de Riscos mapeado, bem como as demais atividades do processo de contratação de TI, e preconiza que deve ser feita a especificação

procedimental do conteúdo de Identificação de Riscos, de maneira abrangente, sem a especificação de critérios objetivos. Essa percepção no processo foi encontrada por não ter sido localizada uma metodologia de identificação dos riscos mensurável no Guia de Contratações de TI. A abordagem desse problema é o tema central do presente trabalho e será detalhado na revisão bibliográfica.

Vale notar que tal questão é indissociável da questão da rastreabilidade dos riscos e o seu monitoramento até a entrega da solução contratada. A carência de aportes teóricos e práticos para essa atividade tem por consequência potencial a utilização de indicadores equivocados para medição e controle de riscos na fase de gestão contratual. Falhas na gestão dos riscos durante os contratos tipicamente se refletem em novas contratações, corretivas ou adicionais, utilizando então mais recursos públicos simplesmente por que a identificação dos riscos necessários não foi prevista da maneira correta por falta de metodologia que permita a seleção de critérios objetivos para identificação de riscos.

O atual modelo de Análise de Riscos solicita que se preencham os riscos sob duas perspectivas: da solução de TI e do processo de contratação de TI. O modelo propõe o preenchimento dos riscos da contratação de TI, contendo os seguintes campos: risco identificado, dano, impacto, responsável, probabilidade, ação preventiva e de contingência.

Ou seja, o modelo de Análise de Riscos da contratação de TI não possui um “fio condutor” para se identificar riscos. A avaliação e tratamento sob a ótica de mensuração do dano, impacto, responsável, probabilidade, ação preventiva e de contingência (gestão de riscos proposta pelo modelo) teoricamente só poderiam ser aplicados após todos os riscos estarem identificados sob todas as possíveis perspectivas. Do contrário, a maneira atual poderá estar avaliando riscos originados de um critério de identificação indefinido, parcial ou não e integrado às variáveis que permeiam toda a contratação. Além disso, não existe um alinhamento formal ou referenciado do modelo de Análise de Riscos da APF à luz de normas de riscos.

Este cenário gera as seguintes consequências:

1. Elaboração de artefatos e documentos sem uma percepção global do processo de contratação.
2. Devido à previsão incompleta dos riscos, problemas de gestão contratual podem ocorrer nas contratações.

3. Não é possível estabelecer um nível de serviço adequado para a contratação, pois é preciso identificar corretamente os riscos que podem afetar a contratação, antes de tratá-los seguindo a metodologia proposta pelo *template* de Análise de Riscos do Guia.

Sendo assim, foi definido o seguinte problema de pesquisa: **Como identificar os principais riscos que possam comprometer o sucesso de uma contratação TI?**

Para tratar tal tema, este trabalho apresentará algumas definições sobre a Análise de Riscos na IN04 e, depois proporá um detalhamento do processo da IN04, com introdução do desenho de um artefato de Identificação de Riscos, cuja metodologia de construção é descrita, bem como os aspectos da validação analítica e prática da proposta apresentada.

## 1.2 HIPÓTESE

Com o problema de pesquisa definido foi idealizada a seguinte hipótese de pesquisa:

- Um artefato baseado no estado da arte de gestão de riscos poderá otimizar o processo de identificação de riscos da IN04, propondo uma abordagem padronizada.

Essa hipótese de pesquisa será validada ou não após o estudo de caso deste trabalho.

## 1.3 QUESTÕES

O trabalho possui questões de pesquisa inerentes ao estado da arte em gestão de riscos. É necessário antes de se fazer qualquer alinhamento do modelo atual com as normas de riscos, responder às seguintes questões sobre riscos: Quais são os autores? Quais são essas normas que tratam de riscos? Como aprimorar a identificação de riscos utilizando essas referências? Como padronizar a maneira de se identificar riscos nas contratações de TI? Existe uma terminologia generalista para riscos nas contratações de TI? O vocabulário utilizado atualmente está alinhado com as normas internacionais?

Tais questões permitem refletir se atualmente, existe ou não uma referência oficial para identificação de riscos voltados às contratações de tecnologia da informação na APF brasileira, baseada em alguma norma, como ABNT NBR ISO 31000.

## 1.4 JUSTIFICATIVA

Compreender os princípios, processos, atividades e atores do modelo de contratações de TI brasileiro sob a ótica do estado da arte em Gestão de Riscos (GR), mediante a aplicação de métodos acadêmicos e de normas de referência, pode ser uma estratégia viável para melhoria do processo atual de identificação de riscos, pois tal prática é adotada por várias organizações de todo mundo que buscam *compliance* com a GR. Como resultado, há possibilidade de aumento da maturidade das contratações de TI na APF no Brasil, pois a identificação de riscos é uma das principais atividades a serem realizadas em uma contratação de TI.

Considerando que as contratações de TI no Brasil são de alta relevância orçamentária, pois envolvem o uso de muitos recursos financeiros, é possível inferir que um planejamento alinhado com uma adequada identificação de riscos poderá evitar desperdícios e otimizar a prestação dos serviços contratados.

Um dos processos para a consolidação de uma boa governança de TI, segundo Barbosa *et al* (2006), são as contratações de serviços de tecnologia da informação (TI).

Existe assim uma necessidade de monitoramento constante das contratações de TI na APF e a utilização do artefato a ser proposto pode apoiar a maneira de se identificar ameaças e vulnerabilidades, possibilitando assim a definição de riscos com uma orientação mínima de um material de referência, direcionada aos profissionais que atuam no planejamento da contratação.

## 1.5 OBJETIVO GERAL

Desenhar um artefato Identificação de Riscos para o processo de contratação de tecnologia da informação na APF, sob o ponto de vista da Norma 31000.

## 1.6 OBJETIVOS ESPECÍFICOS

1. Analisar o atual processo de análise de riscos realizado na fase de planejamento da contratação de TI na APF.
2. Redesenhar o processo de Identificação de *Riscos* com o uso da ferramenta de modelagem de Processos - *Bizagi Process Modeler*[2].

[2] http://www.bizagi.com

3. Propor um novo artefato de Identificação de Riscos no processo de contratação de TI, para apoio da equipe de planejamento da contratação com a devida harmonização terminológica dos termos e conceitos utilizados atualmente.

## 1.7 METODOLOGIA

Para alcançar o primeiro objetivo específico será exposta uma caracterização descritiva a partir da análise documental dos arquivos oficiais da APF, abordando os conceitos e o processo de contratação de TI.

Alguns trabalhos foram utilizados como referência parcial nesta fase. Cruz (2008) foi usado como parâmetro devido ao enfoque e organização dos dados sobre contratações de tecnologia da informação no setor público. A visão adotada por Motta (2010) também foi considerada, quando de uma análise sobre a estrutura de compras pública brasileira e americana e de Cepik, Canabarro (2010), que se referem a um estudo sobre a Governança de TI na Administração Pública Federal brasileira.

Apesar de Cruz (2008), Motta (2010) e Cepik, Canabarro (2010) não terem focado no assunto de Gestão de Riscos (GR) especificamente, os trabalhos contribuíram para se abordar as contratações sob uma ótica mais detalhada, fato que foi percorrido por este trabalho.

Para o segundo objetivo de pesquisa foi utilizada a ferramenta de modelagem de processos *Bizagi Process Modeler*. Esta ferramenta foi escolhida, pois os arquivos de Processo (BPMN) do Guia de Contratação para Soluções de TI foram gerados com este *software*. O arquivo foi solicitado a SLTI e devidamente ajustado conforme proposta deste trabalho.

No terceiro objetivo de pesquisa foram identificados os termos e conceitos do Guia Prático de Contratações de TI do SISP, bem como o que preconiza a ABNT NBR ISO 31000 com apoio da ferramenta *FreeMind*[3]. As informações foram distribuídas na estrutura de árvore hierárquica (mapas mentais). A escolha do *software FreeMind* foi feita pelo fato da ferramenta ser um programa bastante útil para quem procura um meio efetivo de armazenar e organizar ideias, o que reflete a necessidade neste trabalho, devido a grande quantidade de premissas. Em seguida, os termos foram devidamente harmonizados

[3] http://freemind.sourceforge.net/wiki/index.php/Main_Page

terminologicamente, de acordo com normas de vocabulário mundialmente utilizadas para gestão de riscos.

Este artefato foi utilizado para um estudo de caso, onde foi possível verificar sua aplicabilidade em um caso real, de uma contratação já realizada, que teve os riscos novamente identificados, mas agora utilizando o artefato proposto neste trabalho. Essa contratação sob uma nova ótica permitiu a extração de dados que possibilitaram a comparação dos dois cenários de identificação de riscos (anterior e proposto).

## 1.8 DELIMITAÇÃO DA PESQUISA

A seguir a definição de escopo para esta pesquisa:

- Inicialmente a pesquisa possui uma delimitação metodológica em consequência da baixa quantidade de referências e trabalhos similares, além de ser um assunto pouco abordado e recente no meio acadêmico, conforme levantamento preliminar realizado.

- Também como delimitação da pesquisa está o conteúdo pesquisado sobre riscos. Ele é o limite da pesquisa e serão usadas como referência as normas ABNT NBR ISO 31000 - Gestão de Riscos - Princípios e Diretrizes, ABNT NBR ISO GUIA 73 - Gestão de Riscos - Vocabulário e ABNT NBR ISO 31010 - Gestão de Riscos - Técnicas para o processo de avaliação de Riscos.

- O trabalho apresenta uma visão de como se identificar riscos sob a ótica da ABNT NBR ISO 31000, que futuramente poderá ser completada com outros autores, modelos e normas.

- Não é escopo deste trabalho alterar a maneira de se contratar TI, mas sim mostrar uma nova reflexão sobre a identificação de riscos, para que em seguida, seja feito o processo de avaliação de riscos, e não somente de análise, conforme preconiza a ABNT NBR ISO 31000.

- Este trabalho propõe um modelo abrangente, que poderá ser seguido para qualquer contratação de TI, entretanto, guardadas as devidas proporções, é possível que contratações mais complexas possam não ter seus riscos suficientemente identificados devido às particularidades de cada objeto de contratação. Por isso se trata de um modelo genérico, que não tem a intenção de resolver todas as lacunas de identificação de riscos.

- Não irá aprofundar na legislação quem embasou as contratações (lei 8.666/93, Decreto 7.174/2010, Decreto 10.520/2002, dentre outros).

## 1.9 RESULTADOS ESPERADOS

Em consequência da utilização prática do trabalho apresentado, são resultados esperados para as contratações de TI no âmbito da APF:

- Identificação mais completa dos riscos na contratação;
- Visualização e percepção de itens que impactam as contratações, mas que não são gerenciadas por desconhecimento;
- Melhor definição de níveis de serviço;
- Cláusulas contratuais que previnam erros na gestão de contratos;
- Incentivo à melhoria do detalhamento dos riscos pelo órgão;
- Maior envolvimento dos interessados, que poderão perceber impactos;
- Melhor gestão do processo de contratação;
- Menor gasto com as contratações, aliado a melhor qualidade possível;
- Diminuição do gasto público (comprar bem e não somente o mais barato).

## 1.10 ORGANIZAÇÃO DO TRABALHO

Para construção do trabalho, será realizada no capítulo 2 e 3, uma revisão de literatura mais atualizada e disponível possível, das áreas relacionadas a:

- Contratações de TI (Capítulo 2);
- Riscos (Conceitos e Visões) e Normas de Riscos (Capítulo 3)

No Capítulo 4 serão apresentados os mapas mentais com as premissas de riscos que irão gerar o artefato de Identificação de Riscos, bem como a harmonização terminológica e o artefato de identificação de riscos.

No Capítulo 5, será feita a validação e o estudo de caso do artefato de Identificação de Riscos.

No Capítulo 6, as conclusões e recomendações do estudo, indicando quais os possíveis caminhos a serem seguidos a partir deste trabalho.

# 2. REVISÃO DE LITERATURA - CONTRATAÇÕES DE TI

No contexto do gasto público de TI, Cruz (2008), propôs o quadro referencial normativo (QRN) para apoio aos gestores de TI, na busca da diminuição das chances de ocorrência de eventos como a falta de informação, negligência e imperícia dos gestores. O autor aponta que várias organizações públicas não tinham estratégia formal e definida e frequentemente não consideravam uma análise de riscos ou o valor agregado ao negócio, sob a ótica das contratações de TI. Segundo Cruz (2008), isto sugere examinar os métodos empregados para decidir pela contratação de serviços e quais os riscos envolvidos, no contexto do setor público.

Mas quando se fala em contratar TI, diversas variáveis podem influenciar o processo de contratação. Especificação técnica, fornecedores, qualificação dos gestores, comunicação, partes interessadas, áreas correlatas, clientes internos, clientes externos, acordos de nível, serviços, contratos de serviço, etc. Trata-se de uma visão holística de todo o processo e não somente especificar e aguardar o fornecedor vencedor. Essas variáveis são pontos que devem ser controlados e possuem riscos associados, que geram impactos (positivos ou negativos) em algum ponto do processo, caso a questão identificada não seja devidamente tratada.

Barbosa *et al.* (2006) afirmam que para diminuir os riscos identificados nas contratações de TI no setor público são necessários processos e modelos bem estruturados de contratação. Atualmente o Brasil possui uma iniciativa nessa linha, que foi proposta pela Secretaria de Logística e Tecnologia da Informação (SLTI), do Ministério do Planejamento, Orçamento e Gestão (MP). Este trabalho é o Guia Prático para Contratação de Soluções de TI, que possui o desenho do processo de contratação de TI da APF (SLTI, 2011).

Paralelo a esse trabalho de melhoria das contratações, existe o mercado de prestação de serviços de TI. Essas empresas buscam, naturalmente, o maior lucro possível, pois são criadas para esse fim. Estão, por isso, organizadas para apresentar todas as possibilidades para vender seus bens e serviços e isso inclui a carteira de clientes governo, leia-se APF, para esse contexto.

Com o lançamento acelerado de novas tecnologias, compradores públicos que atuam na área de TI dos órgãos ficam cada vez mais interessados em realizar contratações que possam obter o melhor produto aliado ao melhor preço. Entretanto, devem ser

considerados muitos fatores para se julgar uma contratação como eficiente. Um estudo realizado por Motta (2010) mostra que nem sempre uma aquisição mais barata é a melhor compra.

Motta (2010) discute a questão das compras públicas no âmbito da administração direta do poder executivo federal brasileiro com o objetivo de analisar a contribuição deste sistema de compras na busca de maior eficiência do gasto público federal. Foram utilizados conceitos originados da iniciativa privada e do sistema de compras federais norte-americano.

Para o autor, o sistema federal de compras públicas do Brasil, tem maior preocupação com o combate à corrupção e com a legislação e pormenoriza os sistemas e as pessoas, priorizando, por último, o resultado, quando passível de ser identificado.

Assim, considerando a ideia de Motta (2010), que retrata que o resultado pode não ser o fator mais importante das aquisições no país, é possível perceber que no segmento de TI, essa hipótese pode ter um fundamento lógico. Afinal, fabricantes e prestadores de serviços de TI deixam os profissionais da equipe de contratação de TI sempre inquietos com a rápida evolução e oferta de produtos, que caso não sejam substituídos, geram dependência do fornecedor, como falta de garantia e falta de suporte, problemas com versão de *software*, descontinuidade tecnológica, dentre outros.

Portanto, compradores públicos que não avaliam o impacto que a organização recebe desses critérios de mercado, podem buscar melhorias muitas vezes desnecessárias, não orientadas a resultado, mas sim na atualização tecnológica, forçada pelo mercado altamente competitivo e agressivo em vendas. Nesse contexto, deve-se entender todo processo para identificar riscos em vários aspectos, permitindo que as aquisições sejam corretamente especificadas (Planejamento da Contratação), devidamente selecionadas (Seleção do Fornecedor) e gerenciadas por indicadores previamente planejados (Gestão Contratual).

## 2.1 CONTEXTO DAS CONTRATAÇÕES DE TI NA APF

Em 2006, o TCU recomendou à Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MP) que elaborasse um modelo de licitação e contratação de serviços de informática para a APF e promovesse a

implantação nos diversos órgãos e entidades sob sua coordenação mediante orientação normativa. Assim a SLTI publicou a IN04 de 19 de maio de 2008 (atualizada em 2010 e 2012, conforme mencionado na introdução deste trabalho, página 9). A IN04 da SLTI dispõe sobre o processo de contratação de serviços de TI pela APF direta, autárquica e fundacional. A norma contemplou as fases de planejamento da contratação, seleção do fornecedor e gerenciamento do contrato e entrou em vigor no dia 2 de janeiro de 2009 (TCU, 2008).

Além disso, outros fatos aconteceram e estão descritos na Tabela 2-1, refletindo pontualmente os últimos 11 anos de evolução das contratações de TI.

**Tabela 2-1** Contexto histórico das contratações de TI dos últimos 11 anos (Adaptada de CRUZ; ANDRADE; FIGUEIREDO, 2011).

| Ano | Marco |
|---|---|
| 2001-2005 | Processo formal de contratação de bens e serviços de TI proposto pelo TCU (Hernandes) |
| 2006 | Acórdão 786/2006 TCU - Recomenda à SLTI a criar um modelo de licitação e contratação de serviços de informática para a APF |
| 2007 | QRN - Quadro Referencial Normativo, com diversos corolários e legislações de apoio aos gestores de TI (CRUZ, 2007) |
| 2008 | Publicação da IN04 pela SLTI |
| 2008 | Publicação da EGTI. |
| 2008 | Criação da Gratificação Temporária do Sistema de Administração dos Recursos de Informação e Informática (GSISP), que atraiu servidores de outros órgãos para atuarem com gestão de TI. |
| 2009 | Criação dos cargos de Analista de Tecnologia da Informação (ATI) para APF (MP). |
| 2009 | Implantação do Programa de Desenvolvimento de Gestores de TI (DGTI) na ENAP |
| 2009 | Revisão da EGTI 2008 |
| 2010 | Publicação da EGTI 2010 |
| 2010 | Revisão da IN04 |
| 2011 | Publicada EGTI 2011-2012 |

| | |
|---|---|
| 2011 | Versão final do Guia Prático para Contratação de Soluções de TI |
| 2012 | Revisão da IN04 |
| 2012 | Lançamento do Guia de Contratações do TCU, com ênfase em riscos da contratação |

Os autores Cruz; Andrade; Figueiredo (2011) afirmam que há uma diretriz clara no sentido de que as organizações públicas definam e institucionalizem seus processos de contratação de serviços de TI. Eles corroboram que a identificação dos requisitos necessários, a garantia da qualidade dos resultados esperados, os critérios de aceitação, a gestão de mudanças, as transferências de conhecimentos, a legislação pertinente, entre outros aspectos, são pontos fundamentais a serem considerados para as contratações de TI.

Tais questões envolvem também relacionamento entre clientes e fornecedores, o que implica em competências administrativas e jurídicas (CRUZ; ANDRADE; FIGUEIREDO, 2011). Essas complexidades apresentam riscos para as partes envolvidas e podem gerar conflitos. Normas e modelos de referência podem ser úteis para resolver esses conflitos. Assim, um modelo de identificação de riscos da contratação, baseado em normas de referência, permitirá uma visão mais ampla de se identificar potenciais problemas, enriquecendo o método atual, com novos procedimentos.

## 2.2 GOVERNANÇA DE TI APLICADA NAS CONTRATAÇÕES DE TI

Segundo levantamento do TCU no Acórdão 1.603/2008 existem lacunas que podem ser aprimoradas nas Contratações de Tecnologia da Informação.

Neto (2011) trata a questão da Governança de TI como um *Wicked Problem*, termo que pode ser considerado para as Contratações de TI. *Wicked Problems* são questões complexas, dificilmente reconhecidas devido à sua interdependência. Quando *Wicked Problems* são vistos de forma pragmática, o desafio torna-se ainda mais complicado. É necessária uma mudança na mentalidade, percepção das dificuldades de maneira holística, além de habilidades gerenciais para aplicar estratégias e ferramentas de maneira correta para aumentar as chances de resolução dessas questões nas organizações (WEBBER; KHADEMIAN, 2008).

Com esse panorama das contratações de TI, observa-se que é composto por processos e artefatos definidos para se atingir um resultado final. Por isso é notório que a atividade de

se planejar uma contratação demanda pesquisa e conhecimento, além de experiência do gestor. Isso para que o gestor possa com seu trabalho, realizar o "recorte" de quais fornecedores tem condição de fornecer o produto ou serviço mais adequado para APF.

A Figura 2-1 apresenta as interfaces da governança das contratações de TI.

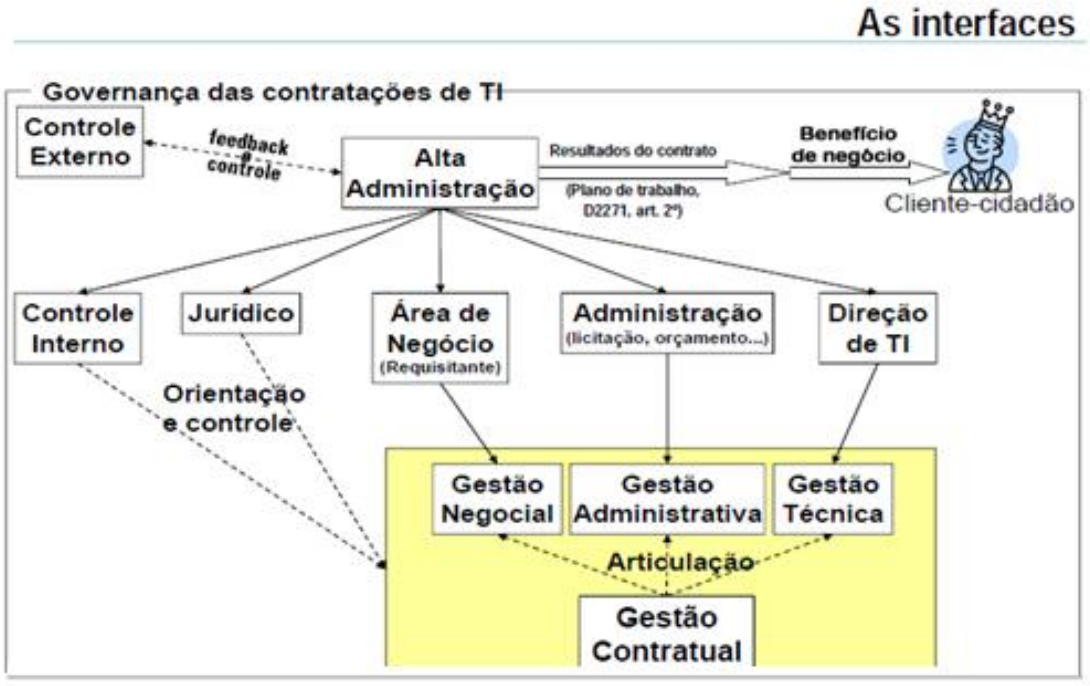


Figura 2-1 Interfaces da governança nas contratações de TI. (Adaptada de CRUZ, 2011a).

Um dos riscos que ocorre nas interações de cada uma dessas interfaces é a questão da comunicação. O controle externo irá adotar ferramentas, acórdãos, leis e penalidades aos infratores das regras estabelecidas para as contratações. Já a alta administração dos órgãos, irá submeter essas diretrizes às áreas internas para que elas sejam de fato seguidas. Ocorre que isso nem sempre pode acontecer, e as áreas inferiores podem não estar cientes das responsabilidades, devido ao conflito mudo causado entre órgãos de controle, alta administração do órgão e áreas de negócio, TI, jurídica, dentre outras. O repasse do conhecimento pode não acontecer, mesmo que as informações sejam públicas, caso as áreas não busquem se atualizar. Isso pode gerar cobranças dos órgãos de controle que muitas vezes sequer estão sendo monitorados, seja por sobrecarga de trabalho dos servidores ou mesmo por falta de treinamento. Diversos fatores podem influenciar nas rotinas de uma contratação de TI, incluindo os riscos de o processo não finalizar por penalidades aos gestores pelos órgãos de controle em qualquer uma das fases da

contratação. As solicitações do mercado podem inclusive atrapalhar as contratações do órgão, caso não tenham efetivamente interesse verdadeiro.

Voltando ao descrito na Figura 2-1 é possível perceber a relevância do processo, que envolve desde o cliente-cidadão até os órgãos de controle externo. É possível também verificar com essa imagem que, apesar da pesquisa propor uma melhoria do modelo de GR atual do processo de contratação, ele é apenas uma parte de todo o processo. Uma contratação bem realizada por si só não garante todos os objetivos. Mas para que ela aconteça, o gestor responsável deve contar também com o empenho das demais áreas envolvidas. Por isso é interessante a responsabilização e definição de papéis de todos os elementos dessa figura e não somente do grupo que especifica a solução.

Cruz (2008) completa que as contratações de serviço de TI no setor público têm ainda as seguintes características:

- É uma opção estratégica da área de TI;
- Afeta diretamente a qualidade dos serviços de TI oferecidos aos clientes;
- A área de TI continua a ser responsável pelos resultados dos serviços contratados;
- Afeta os custos da área de TI e, portanto, o valor agregado à organização;
- Expõe a organização a muitos riscos adicionais (CRUZ, 2008 *apud* WRIGHT, 2004).

Tais questões mostram a relevância do assunto e a influência que a área de TI exerce sobre as organizações. Isso mostra que, no setor público, a contratação de serviços de TI não é uma opção, mas sim o caminho a ser seguido por força do Decreto-lei 200/1967, art. 10, § 7º e da sua regulamentação constante do Decreto 2.271/1997 (CRUZ, 2008).

## 2.3 SISTEMA DE COMPRAS PÚBLICAS DO BRASIL

Motta (2010) conclui em seu estudo que o sistema brasileiro de compras não contribui substancialmente para a melhora da eficiência do gasto público federal. Mas em termos organizacionais, o grande avanço dos últimos anos nos Estados Unidos (EUA) foi fruto da criação, em todas as agências federais, do cargo de *Chief Acquisition Officer* (CAO), de livre provimento.

O autor constata que a abordagem das compras públicas federais no Brasil, mescla o rigor ritualístico a uma onda de destaque para a tecnologia e não para o resultado.

Isso demonstra que a preocupação do estado brasileiro é voltada mais para a formalização de procedimentos do que efetivamente para resultados. Motta (2010) ainda descobriu que, no caso brasileiro, o recrutamento de pessoas frequentemente não leva em consideração a disposição dos servidores em trabalhar em tais áreas, e isso envolve a área de TI.

É de conhecimento na APF o baixo interesse dos servidores em atuarem nos setores de licitações e gestão de contratos, dados os elevados riscos pessoais, os raros, quando não inexistentes, incentivos salariais pelo desempenho, além de fatores como treinamentos insuficientes aliados à forte pressão dos escalões superiores. Esses por sua vez, nem sempre consideram a complexidade advinda da legislação em vigor e finalmente o pouco valor dado aos servidores que desempenham atividades administrativas. Mas tal situação assume contornos mais graves quando contrastada com as áreas de fiscalização e controle, em que existe carreira própria, concurso específico, remuneração adequada e valorização do servidor (MOTTA, 2010).

## 2.4 LEGISLAÇÃO APLICADA AS CONTRATAÇÕES DE TI

A legislação aplicada às contratações de TI é ampla e possui várias normas, leis, decretos, instruções normativas, portarias, acórdãos, notas técnicas, súmulas dentre outros instrumentos que provem informações para quem atua com as contratações.

Guarda (2011) realizou em sua pesquisa uma compilação de normas com sua breve descrição. Essa referência é apresentada na Tabela 2-2, para apresentar o contexto jurídico/normativo no qual estão inseridas as contratações de TI.

**Tabela** 2-2 Normas Federais aplicadas às contratações de TI. (Adaptada de Guarda, 2011)

| | Norma | Data | Descrição |
|---|---|---|---|
| 1 | Lei nº 8.248/1991 | 23/10/1991 | Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências. |
| 2 | Lei nº 8.666/1993 | 21/06/1993 | Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração |

| | | | |
|---|---|---|---|
| | | | Pública e dá outras providências. |
| 3 | Dec. n° 7.579/2011 | 11/10/2011 | Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal. |
| 4 | Dec. nº 2.271/1997 | 07/07/1997 | Dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências. |
| 5 | Dec. nº 3.555/2000 | 08/08/2000 | Aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns. |
| 6 | Dec. n° 3.931/2001 | 19/09/2001 | Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e dá outras providências. |
| 7 | Lei nº 10.520/2002 | 17/07/2002 | Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências. |
| 8 | Lei nº 11.077/2004 | 30/12/2004 | Altera a Lei nº. 8.248, de 23 de outubro de 1991, a Lei nº. 8.237, de 30 de dezembro de 1991, e a Lei nº. 10.176, de 11 de janeiro de 2001, dispondo sobre a capacitação e competitividade do setor de informática e automação e dá outras providências. |
| 9 | Dec. nº. 5.450/2005 | 31/05/2005 | Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências. |
| 10 | Dec. nº. 5.504/2005 | 05/08/2005 | Estabelece a exigência de utilização do pregão, preferencialmente na forma eletrônica, para entes públicos ou privados, nas contratações de bens e serviços comuns, realizadas em decorrência de transferências |

| | | | |
|---|---|---|---|
| | | | voluntárias de recursos públicos da União, decorrentes de convênios ou instrumentos congêneres, ou consórcios públicos. |
| 11 | IN n° 02 MPOG/SLTI | 30/04/2008 | Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não. |
| 12 | Portaria n° 11 SLTI | 30/12/2008 | Define a Estratégia-Geral de Tecnologia da Informação para a Administração Pública Federal. |
| 13 | Dec. n° 7.063/2010 | 13/01/2010 | Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas do Ministério do Planejamento, Orçamento e Gestão, e dá outras providências. |
| 14 | Dec. nº 7.174/2010 | 12/05/2010 | Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União. |
| 15 | IN n° 04/10 MPOG/SLTI | 16/11/2010 | Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. |

Esse compilado das legislações serve para contextualizar este trabalho, que tem como objetivo propor um artefato para identificar riscos, que irá contribuir com o atual modelo de Análise de Riscos proposto pelo Guia Prático de contratações do SISP. Portanto, não será objeto do presente estudo a exploração detalhada das normas.

## 2.5 RESPONSABILIDADE, GESTÃO PÚBLICA E GOVERNANÇA

Segundo orientações da ABNT NBR ISO 38500, que trata de governança corporativa e de TI, todos da organização devem compreender e aceitar suas responsabilidades, no que diz

respeito às demandas de TI. Esse conceito é vinculado ao princípio da responsabilidade da norma (ABNT, 2009c).

Essa relação também é válida para cliente/fornecedor. Eles devem trabalhar em parceria, usando uma comunicação eficaz e com base em relações positivas e de confiança, que demonstrem clareza e responsabilidade (GASETA, 2011).

Cumpre ressaltar que a responsabilidade deve permear toda estrutura organizacional e, para o sucesso das iniciativas, as camadas de alto nível devem ter as iniciativas de governança.

O TCU (2010) reitera que o uso do termo "governança" pode ainda não ser bem compreendido na Administração Pública, por não ser de definição simples e também não deve ser confundido com o termo "gestão". Ambas são atividades distintas e devem ser observadas sob o aspecto tático (Governança) e de controle (Gestão), algumas vezes utilizando aspectos operacionais (Executor).

O controle por sua vez é um dos os pilares da governança de TI, juntamente com valor e risco. Tais critérios compõem a tríade a qual é de responsabilidade dos executivos e da alta direção das organizações garantirem que a TI apoie os objetivos e estratégias da organização (ITGI, 2007). A Figura 2-2 ilustra esse contexto, incluindo as terminologias, que devem ser utilizados nas relações da área de TI com clientes, fornecedores externos e internos, no contexto das contratações de TI.

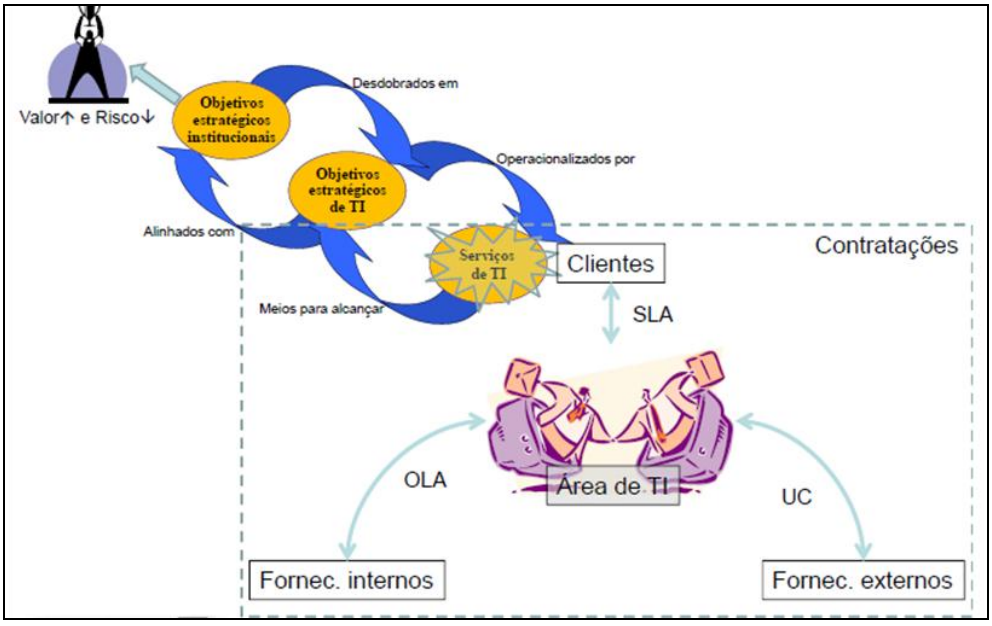


Figura 2-2 Valor, riscos e contratações (relacionamento da área de TI). (Adaptada de CRUZ, 2011a).

Sendo assim, as variáveis de valor e riscos devem ser inversamente proporcionais (maior valor, menor risco) para busca de objetivos estratégicos institucionais mais sólidos, que estejam alinhados com objetivos estratégicos de TI, os quais devem estar operacionalizados por serviços de TI.

Na prestação de serviços de TI, clientes devem ter suas expectativas gerenciadas e monitoradas em acordos de nível de serviço (*Service Level Agreement* - SLA) pela área de TI para que as demandas sejam executadas de acordo com o planejado. Afinal, qualquer coisa diferente do planejado, caso não seja previsto, mesmo que seja uma melhoria, poderá gerar outras expectativas difíceis de serem alinhadas, pois uma contratação de TI não deixa de ser um projeto. Os clientes por sua vez, devem consultar o catálogo de serviço da área de TI para verificar quais os serviços disponíveis (MAGALHÃES; PINHEIRO, 2007).

A criação de um portfólio de TI ou catálogo de serviços é realizada quando a organização já possui claramente alguns serviços que são solicitados pelos seus usuários. A divulgação de um portfólio permite que a TI atue dentro do seu escopo oferecendo aos seus clientes serviços compatíveis com o negócio. Após várias interações, uma área de TI normalmente se adapta para atender as demandas de negócio da organização.

Não possuir um portfólio de TI claro e bem divulgado, impacta na questão de a TI receber demandas que ela muitas vezes não está preparada, mas acredita que pode fazer, refletindo diretamente em sua capacidade operacional e alterando prazos devido à falta de escopo de sua atuação.

Portanto, considerar a criação do portfólio de TI é fundamental para permitir à área de TI delimitar o escopo de atuação para que fique claro aos clientes internos qual seu papel e no que ela pode ajudar. Essa ideia vem ao encontro da Figura 2-2, que apresenta dois objetivos claros: aumentar o valor e diminuir os riscos.

Essa mesma área de TI, para atendimento do nível de serviço com clientes, deve buscar em fornecedores internos, condições de operacionalizar suas soluções, por meio de Acordos de Nível Operacional (*Operation Level Agrement* - OLA). Essa "parceria" permitirá uma aderência correta do nível de serviço com clientes (MAGALHÃES; PINHEIRO, 2007).

Além de fornecedores internos, a TI deve prover por meio de contratos de apoio (CA) com fornecedores externos, as soluções que devem ser suportadas pelas contratadas. Esses

contratos são, na verdade, o produto a ser gerenciado pela área de TI, e onde está o foco desta pesquisa, pois é com o trabalho adequado de planejamento e verificação de riscos que as contratações poderão atingir os níveis de serviços dos clientes, que estão baseados em objetivos estratégicos institucionais (MAGALHÃES; PINHEIRO, 2007).

Para validação, monitoramento e avaliação desse plano da Figura 2-2, a utilização de um comitê de TI em organizações de grande porte, típicas no setor público, composto por vários membros de diversos níveis da organização, presidida por um membro do próprio comitê, é um mecanismo eficaz para avaliar, orientar e monitorar o uso da TI. Priorizar demandas e investimentos, orientar e monitorar o uso da TI é tarefa do comitê de TI que tem como objetivo deliberar sobre atividades de responsabilidade, governança e gestão pública (GASETA, 2011), em nível de órgãos ou mesmo nível de poderes (Executivo, Legislativo, Judiciário).

Nesse cenário, é importante ressaltar que o planejamento no setor público é tratado como um processo de várias etapas como: estabelecer os objetivos e metas, fazer planos, executá-los e tendo como resultado um plano para um futuro determinado (OLIVEIRA, 1996).

## 2.6 GOVERNANÇA NAS ORGANIZAÇÕES PÚBLICAS E PRIVADAS

Um fator que afeta as estruturas de governança tanto no setor público quanto no privado é o grupo de *stakeholders* que as organizações devem satisfazer. O setor privado tem como principal meta maximizar os objetivos financeiros dos proprietários, o mesmo não ocorrendo no setor público. Nesse caso, o grupo de seus *stakeholders* é mais complexo (SUOMI; TÄHKÄPÄÄ, 2004).

A sobrevivência no setor privado tem a ver com a manutenção da organização no mercado. Para os representantes do setor público, a sobrevivência significa poder manter-se, ou manter o seu partido político no poder (PMI, 2002).

Entretanto trazer os conceitos utilizados na iniciativa privada para o setor público pode ser uma tarefa difícil, mas fundamental para avançar na questão das melhorias do uso dos recursos públicos (MOTTA, 2010).

As organizações públicas dependem em maior grau do ambiente sociopolítico do que as empresas, devido à sua estrutura permitir cargos de confiança muitas vezes vinculados a

partidos políticos. Ou seja, seu quadro de funcionamento é regulado externamente à organização. Elas podem exercer autonomia para gerir seus negócios, mas inicialmente, seu mandato vem do governo, sendo os objetivos fixados por autoridade externa. Entretanto, as organizações públicas mantêm as mesmas características básicas das demais organizações, acrescidas de algumas particularidades como: apego às regras e rotinas, supervalorização da hierarquia, paternalismo nas relações, apego ao poder, dentre outros (PIRES; MACEDO, 2006).

Essas diferenças exercem papel importante na definição dos processos internos da organização pública, na relação com mudanças e inovação, na formação de políticas de recursos humanos, contribuindo para os critérios de riscos da organização (PIRES; MACEDO, 2006).

Segundo Barbosa *et al (*2006) as práticas de gestão pública sofrem a influência das tendências e fenômenos sociais, políticos, econômicos e tecnológicos, da mesma forma que as empresas do setor privado. Assim, modelos de gestão praticados no setor privado podem ser adaptados para o modelo de gestão pública, incluindo os mecanismos de governança. A governança engloba a aplicação de conceitos como gestão por resultados, gestão por processos, indicadores de desempenho, gestão por competência e adoção da TI para a transformação organizacional.

A TI tem sido reconhecida como agente de mudança no setor público e como instrumento facilitador das reformas necessárias no setor. A adoção da TI, através de iniciativas de programas de governo eletrônico, por exemplo, criam condições necessárias para a governança (BARBOSA, 2006).

Um problema fundamental ao planejamento e à gestão pública, apontado por Pires e Macedo (2006) é a existência constante de dois corpos funcionais com características bem distintas: um, permanente, é formado pelos servidores de carreira, e o outro, não permanente, é formado por administradores políticos que seguem objetivos externos e mais amplos aos da organização. Existe ainda, outro corpo que é o dos prestadores de serviço, advindos de contratações.

O conflito entre eles é acentuado pela substituição do corpo não permanente a cada novo governo. Este fato é o que mais diferencia uma organização pública da privada, trazendo para a primeira, características como: i) projetos de curto prazo - dura apenas um mandato

para ter retorno político; ii) duplicação de projetos - cada novo governo inicia novos projetos, mesmo que sejam iguais aos da antiga administração, no intuito de reivindicar a autoria para si; iii) conflitos de objetivos - entre os objetivos do corpo permanente e aqueles do não-permanente, que pode levar a pouco empenho para encaminhar ações que vão contra os interesses da corporação; iv) administração amadora - os administradores são pessoas com pouco conhecimento da história e da cultura da organização e, não raro, sem preparo técnico para o exercício da função, pois predomina o critério político de indicação para cargos, em detrimento dos critérios técnicos (PIRES; MACEDO, 2006).

No contexto das contratações de TI, instrumentos como a EGTI (Estratégia Geral de Tecnologia da Informação) e o PDTI (Plano Diretor de Tecnologia da Informação) podem diminuir a ocorrência de muitos fatores de riscos, entretanto, existe ainda liberdade e alguma discricionariedade nos atos desses agentes políticos que podem interferir sobre decisões técnicas, o que pode ser perigoso para as organizações.

A EGTI é um instrumento de gestão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), que estabelece a direção da Tecnologia da Informação (TI), na busca de se definir um plano estratégico, com objetivo de promover a melhoria contínua da gestão e governança de TI, bem como da sustentação da infraestrutura. A EGTI busca atendimento do que determina o Art. 3º da Instrução Normativa (IN) SLTI/MP nº 04, de 12 de novembro de 2010.

O PDTI por sua vez é o instrumento que permite nortear e acompanhar a atuação da área de TI, definindo estratégias e o plano de ação para implantá-las. É uma importante ferramenta de apoio à tomada de decisão para o gestor, habilitando-o a agir de forma proativa, contra as ameaças e a favor das oportunidades.

Segundo Rezende (2004), as organizações públicas obedecem a legislações e enfrentam um ambiente competitivo, turbulento e globalizante. Por isso, necessitam realizar sua reestruturação, adaptações e modificações de forma política, social, ambiental e econômica para poderem continuar presentes e atuantes de forma competente na sociedade; e é nesse contexto que o papel da TI terá que ser revisto. Ainda segundo o autor, nas organizações públicas as dificuldades de alinhar o Planejamento Estratégico Institucional de Sistemas de Informação ao Planejamento Estratégico são maiores do que na iniciativa privada, tendo em vista as mutações políticas constantes. As dificuldades encontradas estão relacionadas

como o clima organizacional não totalmente ativo, com o plano de carreira estático que dificulta a prática efetiva da governança de TI, além do fato de que a estrutura organizacional e suas infraestruturas sofrem mutações mais frequentemente, prejudicando seus planejamentos.

De acordo com Gaspar (2005, p. 21), o governo deve ser aberto e democrático, e assim, requer uma quantidade de controles e cuidados nos gastos bastante significativos. Por isso seus movimentos são mais lentos comparando-se aos das empresas.

Sendo assim, o maior desafio dos gestores públicos é fazer com que a TI desempenhe o papel relevante para a estratégia nas organizações públicas, agregando valor aos seus serviços e diminuindo riscos em todos os sentidos, não somente os das contratações, que são apenas um ponto de todo processo de governança das organizações.

## 2.7 GASTOS DE TI NA APF

Com a evolução das cadeias de logística e abastecimento da economia brasileira nos últimos anos, muitas empresas puderam ter a oportunidade de fornecer ao governo seus produtos e serviços. Paralelo a esse crescimento é cada vez mais comum notícias de superfaturamento, compra indevida ou simplesmente má gestão do recurso público. O estudo de Motta (2010) aponta que o sistema brasileiro de compras não contribui substancialmente para a melhora da eficiência do gasto público federal.

Motta (2010) verificou em sua pesquisa que a corrupção passiva responde por maior parte dos erros de gestão (83%). Esse estudo foi realizado na Itália, entre 2000 e 2005, mas provoca uma necessidade de análise crítica, pois é possível melhorar a gestão das contratações no Brasil, país que possui significativos níveis de corrupção.

Isso significa que seria possível economizar muito mais e melhorar a eficiência da máquina pública caso houvesse um planejamento mais eficiente das contratações, seja de tecnologia da informação ou de qualquer outro segmento.

O uso de recursos públicos envolve muitos fatores, dentre eles a questão ética do servidor público, designado para exercer seu trabalho de gestão. Entretanto, essa é somente uma das características, se considerarmos que esse tema pode ser abordado sob uma visão de melhoria de políticas públicas e outra visão voltada para execução das atividades dos recursos públicos (MOTTA, 2010).

É cada vez maior a cobrança dos órgãos de controle na área de TI, uma vez que essa é uma área muito crítica para obtenção de resultados institucionais (TCU, 2010).

Gerenciar recursos de maneira adequada não é tarefa fácil. É necessário que as pessoas estejam preparadas para gerir o dinheiro público com responsabilidade, transparência e aderência às necessidades de negócio da organização.

## 2.8 ALINHAMENTO DA TI E PLANEJAMENTO ESTRATÉGICO

No levantamento de auditoria efetuado pela Secretaria de Fiscalização de Tecnologia da Informação (SEFTI/TCU), junto a diversos órgãos e entidades da APF, com vistas a obter informações acerca da governança de Tecnologia da Informação (TI), foi verificado que no ano de 2008, 47% dos órgãos pesquisados não possuíam planejamento estratégico institucional em vigor e 59% não fazem planejamento estratégico de TI. A falta de planejamento, segundo o Tribunal de Contas da União, afeta diretamente a eficácia e a efetividade das propostas orçamentárias e das contratações de bens e serviços de informática (TCU, 2008).

O Planejamento Estratégico e Institucional de TI apoia a organização a alocar os recursos públicos conforme as necessidades e prioridades (TCU, 2010).

O COBIT 4.1, em seu processo PO1, sugere a definição um Plano Estratégico de TI, pois ele é necessário para gerenciar todos os recursos de TI em alinhamento com as prioridades e estratégias (ITGI, 2007).

Os indicadores de planejamento estratégico do governo apresentam uma visão de outras esferas, mas destaca-se para esse trabalho apenas as instituições que fazem parte do SISP, pois estes devem seguir as diretrizes da EGTI, assim como usar o Guia Prático para Contratação de Soluções de TI.

O SISP tem o seguinte objetivo, segundo Cepik; Canabarro (2010):

> Planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de informação e informática dos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, em articulação com os demais sistemas que atuam direta ou indiretamente na gestão da informação pública federal.

A Figura 2-3 apresenta a evolução das organizações do SISP, no que tange à criação do Planejamento Estratégico e Institucional de TI.

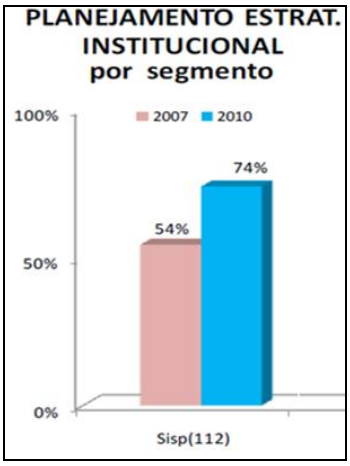


Figura 2-3 Planejamento Estratégico Instit. dos órgãos do SISP (2007 e 2010). (Adaptada de TCU, 2010).

Nesse contexto em que a tecnologia da Informação ocupa um papel essencial no apoio do negócio da organização é importante destacar que o Planejamento Estratégico de TI deve ser elaborado com base no Planejamento Estratégico Institucional, pois este sim reflete o negócio e as necessidades da organização, da qual a TI poderá prover recursos para apoio ao negócio. A criação de um comitê de TI para deliberação de decisões importantes, também é uma boa prática que deve ser adotada pelas organizações que desejam evoluir seu nível de governança de TI, conforme já dito em sessões anteriores.

Planejar as contratações de TI em harmonia com o Planejamento Estratégico Institucional e com o Plano Estratégico de TI, já está consolidado por diversas jurisprudências do TCU (Acórdãos nº 1.521 e 1.558/2003, 2.094/2004, 786/2006 e 1.603/2008).

A ausência de PDTI sugere que há contratações de TI sendo empreendidas em desacordo com a legislação e jurisprudência, segundo o TCU (2010) e a IN04.

Isso sugere que desse percentual de organizações, qualquer aquisição feita por elas sem esse plano, poderá ser considerada como uma tentativa com alto risco de se resolver um problema que mal se sabe o que é apesar dele estar visível e aparente, mas teoricamente "não documentado ou justificado". Independentemente da solução, a aquisição tem chances de ser não ser bem sucedida. É uma solução para um problema não identificado.

Assim, o alinhamento da TI com o negócio é uma atividade fundamental devido à dinâmica dos seus ambientes, segundo Brier (1999). Essa abordagem se torna complexa, levando muito tempo para se desenvolver e ainda mais para se sustentar.

O alinhamento entre o planejamento de TI e os planos de negócio da organização deve ser uma realidade também no serviço público e, para tanto, é preciso haver uma negociação bilateral nesse alinhamento estratégico entre a área de TI e a organização.

Desta forma, o alinhamento com acordos bilaterais facilita e possibilita que decisões de investimentos sejam tomadas com mais clareza, reduzindo risco de erros.

A Figura 2-4 pode apoiar a justificativa que para a TI existir, ela deve estar embasada em uma estratégia de negócio, para então se contratar algo, baseado em seu PDTI. Na figura, verifica-se um dado crítico para o contexto do trabalho: 63% das organizações não tinham aprovado nem publicado seu PDTI em 2010 (TCU, 2010).


Figura 2-4 Deficiências relevantes em governança e gestão de TI. (Fonte: TCU, 2010).

## 2.9 PROCESSO DE TRABALHO E PLANEJAMENTO PARA CONTRATAÇÕES

Nas contratações de Tecnologia da Informação, bem como nas demais regidas pela lei de licitações, é vedado aos gestores à especificação de bens, salvo nos casos em que for tecnicamente justificável, a inclusão de bens e serviços sem similaridade ou de marcas, características e especificações exclusivas (BRASIL, 1993). Ou seja, de maneira geral, não se pode dizer pontualmente o que se deseja comprar, mas devem-se citar as características do produto/serviço, para que o mercado sintetize a "quebra" do conceito do produto/serviço e assim, caso possua o produto, participe da licitação.

Essa prática gera muitas interpretações e especificações diferentes, pois cada gestor pode fazer de um jeito diferente sua descrição do item a ser comprado, contribuindo para uma complexidade maior da contratação.

Em geral o processo de trabalho para aquisição de bens e Serviços de Tecnologia da Informação era apenas a lei de Licitações (BRASIL, 1993), segundo o Acórdão 2.308/2010 – TCU.

A IN04 com sua atualização em 2010 contribuiu para uma melhor compreensão dos conceitos abordados quanto ao processo de trabalho de aquisição de bens e serviços de TI.

Já o COBIT 4.1, em seu processo AI5.1 Controle de Aquisição, sugere que a organização deve desenvolver e acompanhar um conjunto de procedimentos e padrões com o processo e a estratégia corporativa de aquisição, a fim de assegurar que a aquisição de TI satisfaça aos requisitos de negócio (ITGI, 2007).

As justificativas dos benefícios de negócio que uma contratação de TI pode prover devem estar claramente definidas, para não gerar dúvida quanto à necessidade de uma contratação. Mas, segundo levantamento do TCU, menos da metade das instituições costumava explicar os benefícios de negócio, até o ano de 2008 (TCU, 2008).

A maior preocupação apontada, é que a Administração não planeja suas contratações de TI seguindo processos de trabalho formais e definidos (TCU, 2010). Isso mostra que a falta de Governança de TI das instituições que contratam é ainda crítica.

## 2.10 AUDITORIAS NA GESTÃO DE CONTRATOS DE TI

Realizar uma gestão contratual coerente, com um planejamento da contratação não aderente às necessidade reais de negócio, previamente planejadas é uma contradição. De nada adianta gerir um contrato com métricas desproporcionais ou incompatíveis com a realidade do órgão. Isso leva a um número cada vez maior de auditorias por parte dos órgãos de controle.

Sejam auditorias internas ou externas, esse número é elevado (TCU, 2010). No caso das auditorias de TI, a Figura 2-5 apresenta um panorama de alguns indicadores:

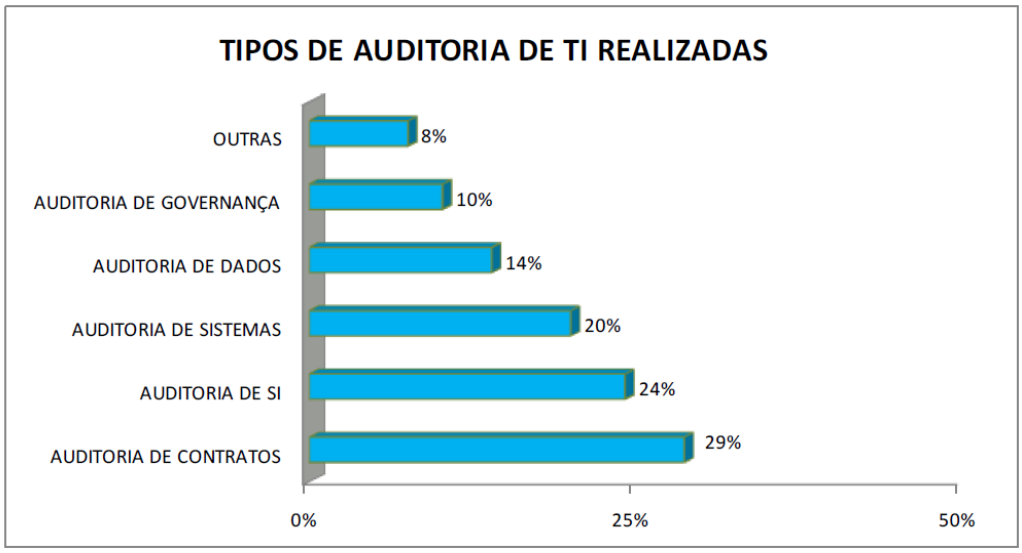


Figura 2-5 Evolução dos indicadores de auditoria de TI. (Fonte: TCU, 2010).

Como as auditorias têm como premissa que aquele que realizou o trabalho não tem condições para auditar o mesmo, é recomendado que nos casos em que a organização não possua pessoal qualificado para tal, a contratação de um serviço desse tipo seja uma prática que poderá ser avaliada seguindo critérios de segurança da informação previamente definidos (TCU, 2010).

Esses dados mostram que é preciso planejar melhor e evitar também, riscos de falhas que podem ser encontradas somente em auditorias externas, o que pode causar prejuízos ao gestor e ao órgão caso existam falhas graves.

## 2.11 GESTÃO DE NÍVEIS DE SERVIÇO DE TI

Um número muito preocupante, apontado pelo Acórdão 1.603/2008 - TCU, diz respeito à gestão de acordos de níveis de serviços prestados internamente: 89% das organizações não

realizam esse acompanhamento, inclusive a gestão de contratos de serviços externos (74% das organizações não acompanham).

O TCU expediu também a Nota Técnica 06/2010, que trata da aplicabilidade da Gestão de Nível de Serviço como mecanismo de pagamento por resultados em contratações de serviços de TI pela APF. Essa nota técnica é fundamental para a construção de termos de referência que vinculem as condições de entrega ao pagamento. Ou seja, nunca se deve pagar um fornecedor sem que ele tenha efetivamente prestado o serviço.

O acompanhamento desses níveis permite realizar ajustes e aferimento da qualidade dos serviços de TI em função das necessidades da organização, devendo neles integrar como indicadores, entre outros, a disponibilidade da infraestrutura de rede, o desempenho dos sistemas e o tempo de solução de problemas (TCU, 2008).

Segundo o Acórdão 2.308/2010 - TCU, a gestão de níveis de serviço de TI garante a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização.

Este talvez seja o maior critério de aceitação de qualidade de um objetivo a ser cumprido por uma área de TI, uma vez que o papel da TI é apoio para as organizações. Isso por que a falta desse critério pode aumentar a insatisfação dos clientes além de riscos de perda de investimento devido à falta de alinhamento das aquisições de TI com a necessidade de negócio.

Já o COBIT 4.1, em seu processo DS1, sugere a definição de gerenciar níveis de serviços, para que as organizações possam acompanhar os trabalhos por critérios previamente acordados. Mais do que definir indicadores, a comunicação eficaz entre a alta direção de TI e os clientes internos pode resultar no nível de serviço adequado (ITGI, 2007).

Para uma contratação eficiente e econômica, segundo o Decreto 2.271/97, art. 6º, a qualidade dos serviços recebidos deve ser medida por resultados, bem como o pagamento. Essa é a maior preocupação que um gestor de TI deve ter, uma vez que não existe condição mais adequada para se contratar bem. Ou a contratação é aderente ao negócio da organização ou não. Uma contratação mal elaborada, poderá inclusive gerar outras contratações desnecessárias, gerando assim um ciclo vicioso e improdutivo para a organização.

As contratações não alinhadas ao PDTI podem gerar contratações corretivas e contratações que dão a falsa sensação de que a TI irá apoiar o negócio. Pode acontecer inclusive dessas contratações sequer gerarem indicadores, uma vez que esses iriam anunciar o fracasso da contratação, por mais que o gestor tenha boa fé em resolver um problema que na visão dele, seria relevante para TI, mas não para a organização.

A gestão de acordos de nível de serviço com os clientes internos é um processo que exige conhecimento e experiência e a gestão de níveis de serviços de fornecedores deveria ser uma prática amplamente adotada. A falta de indicadores pode impactar em fornecedores controlando seus próprios níveis de serviço (TCU, 2010).

Nesse contexto, o COBIT 4.1, sugere em seu processo DS 2.2 a Gestão do Relacionamento com Fornecedores, para que seja formalizado o processo de gestão do relacionamento com cada fornecedor. Para isso, deve ser estabelecida a ligação entre os clientes e os negócios dos fornecedores a fim de garantir a qualidade do relacionamento com base na confiança e na transparência (ITGI, 2007). Para o Acórdão 2.308/2010 - TCU Acórdão, indicadores de níveis de serviços podem ser usados para garantir essa transparência.

## 2.12 COMPRAS SUSTENTÁVEIS DE TI

Um cuidado que os gestores de TI devem ter ao se especificar soluções de tecnologia da informação é com a questão da sustentabilidade. As compras públicas no Brasil movimentam cerca de 10% do PIB, o que demonstra o grande poder de indução da Administração Pública nas contratações de maneira geral (MP, 2010).

O poder de compras da Administração Pública Federal possui enormes potencialidades econômicas, sociais e políticas, podendo inclusive desempenhar um papel de destaque na economia, quanto aos padrões do sistema produtivo e do consumo de produtos e serviços ambientalmente sustentáveis incluindo o estímulo à inovação tecnológica (MP, 2010).

A demanda permanente das entidades da APF, nas três esferas de governo, por um amplo conjunto de bens, serviços e obras para o seu funcionamento, implica em um consumo potencial de recursos naturais e causa impacto direto em todas as etapas associadas à produção; transporte; utilização dos produtos; e geração de resíduos ou formas de disposição final (MP, 2010).

Surge então, a necessidade de racionalização das contratações públicas, que devem priorizar a utilização de materiais recicláveis, com vida útil mais longa, que contenham menor quantidade de materiais perigosos ou tóxicos, consumam menor quantidade de matérias primas e energia, e orientem as cadeias produtivas a práticas mais sustentáveis de gerenciamento e gestão.

Com esse movimento por parte do setor público, será uma tendência natural o mercado fornecedor se adaptar a essa realidade, produzindo ganhos em escala.

Mais do que selecionar a proposta mais vantajosa, considerando não apenas o preço, mas a qualidade e o custo deve-se selecionar produtos que protejam e diminuam os danos ao meio ambiente, o que hoje se traduz em uma política de desenvolvimento sustentável.

A seleção de empresas que apoiem o crescimento nacional bem como daquelas que se preocupam com o tratamento dos resíduos sólidos também deve ser uma prioridade do governo, no que tange às contratações públicas. Desde 2010, fabricantes, distribuidores, importadores e revendedores são responsáveis pelo gerenciamento e descarte final de seus resíduos (Lei 12.305 de 2 de agosto de 2010).

Todos os dias mais de 150 mil toneladas de lixo são produzidos nas cidades brasileiras, sendo que, 59% vão parar em lixões (OLIVEIRA, COSTA, 2010). Mais do que uma questão de comprar bem, é uma questão de melhoramento contínuo das políticas públicas. Considerando que comprar bens de tecnologia da informação em geral envolve equipamentos compostos por metais pesados, a preocupação por parte do governo em saber como as empresas tratam seus resíduos é fundamental.

Os gestores devem prever em suas contratações a gestão do lixo residual dos componentes, caso seja uma contratação para aquisição de ativos de TI, tais como computadores, impressoras, *scanners*, cabos de rede, etc. Isso pode ser feito prevendo e planejando o descarte dos equipamentos, ou mesmo, uma doação à entidade que possa fazer o reuso dos componentes quando estes não forem mais de interesse da Administração Pública.

A IN 01/2010, conhecida como “IN Verde”, especifica inclusive em seu primeiro parágrafo:

> Nos termos do art. 3º da Lei nº 8.666, de 21 de junho de 1993, as especificações para a aquisição

> de bens, contratação de serviços e obras por parte dos órgãos e entidades da administração pública federal direta, autárquica e fundacional deverão conter critérios de sustentabilidade ambiental, considerando os processos de extração ou fabricação, utilização e descarte dos produtos e matérias-primas.

Já o art. 7, parágrafo 2:

> Os bens de informática e automação considerados ociosos deverão obedecer à política de inclusão digital do Governo Federal, conforme estabelecido em regulamentação específica.

Para uma abordagem mais completa do roteiro das contratações sustentáveis, deve-se observar o disposto na Cartilha Sustentável, proposta por Oliveira, Costa (2010). A cartilha contém recomendações para implementação de contratações sustentáveis nas organizações públicas, bem como uma metodologia para se implantar compras públicas sustentáveis.

## 2.13 RECURSOS HUMANOS DE TI NA APF

Para Santos (2011) a formação continuada e a reciclagem de gestores de tecnologia da informação (TI) são fundamentais para melhorar a governança na área, sendo um dos pilares, as contratações de TI.

É um problema recorrente a falta de estrutura de pessoal de TI na APF. Existe um quantitativo deficiente de servidores efetivos, com significativo percentual de colaboradores externos em alguns dos principais órgãos da APF. Outro problema também conhecido e crítico é o percentual elevado de funcionários sem formação específica no setor de TI (TCU, 2008).

O risco de perda de conhecimento organizacional assimilado por trabalhadores não compromissados com a instituição, pode causar muito impacto no negócio (TCU, 2008), uma vez que se trata de investimento em quem não irá aplicar o conhecimento para a organização.

A perda de conhecimento e a atribuição de pessoas que não fazem parte do quadro próprio (colaboradores externos) de uma organização pública são fatores que aumentam o risco da TI. Neste contexto, estão inseridos além de terceiros, cargos em comissão que terceiros assumem (TCU, 2010).

O COBIT 4.1, em seu processo PO7.1, sugere o recrutamento e retenção de pessoal, como uma boa prática a ser seguida pelas organizações.

O Acórdão 140/2005-TCU-Plenário, aponta a preocupação com os recursos humanos da área de TI de toda a administração pública.

Já o Acórdão 2.308/2010 - TCU apresenta que o Ministério do Planejamento foi o órgão que mais promoveu o aumento do quantitativo de pessoal quanto às carreiras de TI. Somente entre o período de 2007 até 2010, o índice geral aumentou de 43% para 78%, boa parte devido à influência do Ministério, pela criação de gratificações e carreiras do SISP.

Essa ação contribui para diminuição da rotatividade, conhecimento do negócio e aprendizagem organizacional, o que leva o órgão a amadurecer os conceitos de Gestão de TI e no consequente aumento da governança de TI. A Figura 2-6 apresenta a evolução de indicadores de pessoal de TI em todas as esferas, para contextualizar o quadro da estrutura de pessoal de TI da APF.

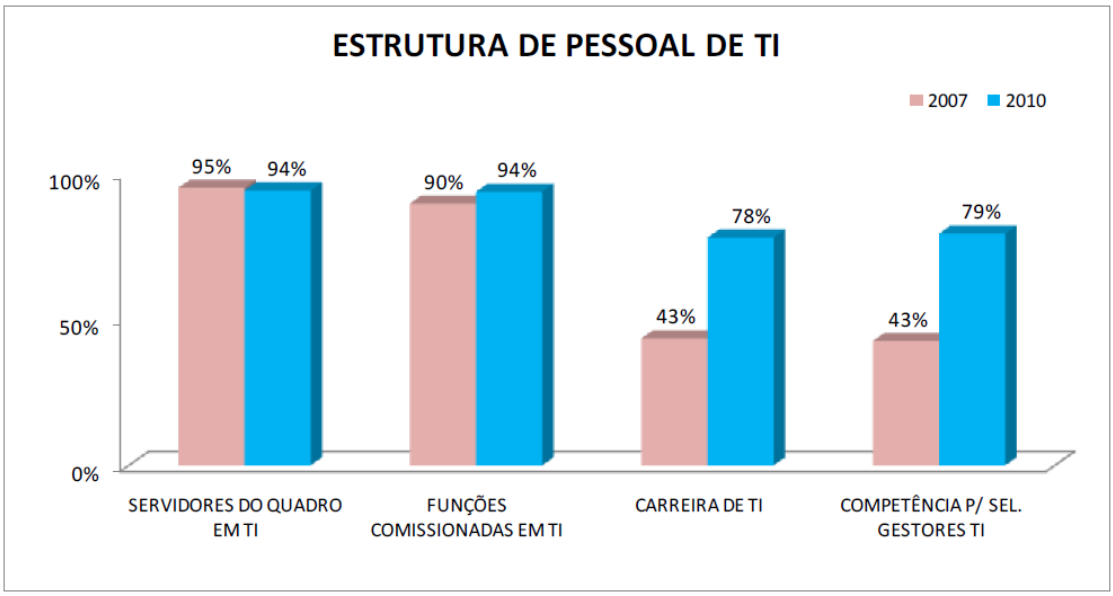


Figura 2-6 Evolução de indicadores de pessoal de TI. (Fonte: TCU, 2010).

Já a Figura 2.7 apresenta os critérios de seleção dos gestores de TI, que muitas vezes é negligenciada e toma por base critério político e pessoal, ao invés de critérios técnicos.

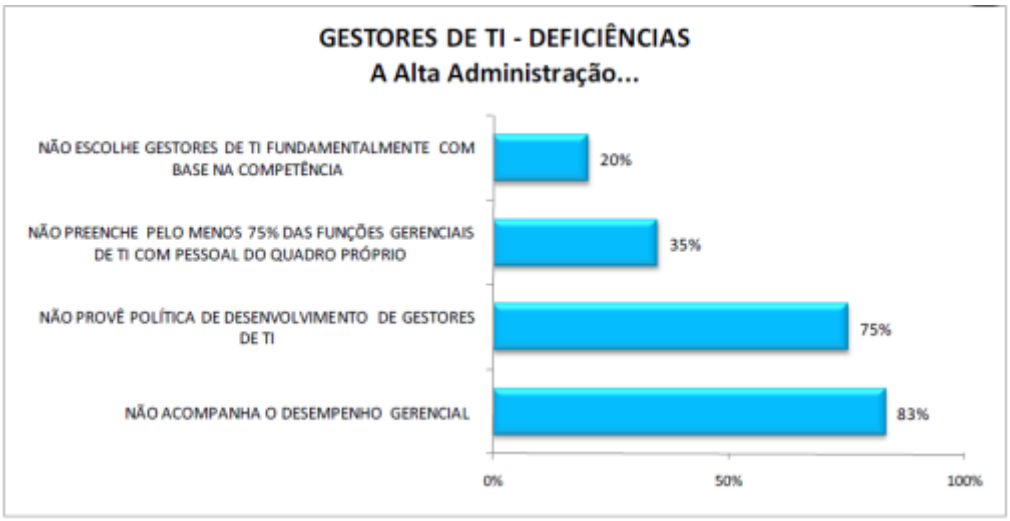


Figura 2-7 Critérios de seleção para gestores de TI. (Fonte: TCU, 2010).

Com esses dados, é possível verificar que a estrutura de compras públicas de TI do estado brasileiro é amadora e sua melhora depende de mudanças que abrangem revisão de regulamentos e de recursos humanos. Este fato é corroborado por Motta (2011). O autor ressalta que para aplicar o conceito no país é necessário, antes, elevar o setor de compras para os cargos de maior hierarquia da administração pública, e isso inclui as compras de TI.

Essa é uma característica tanto da iniciativa privada quanto do governo norte-americano, que há muito tempo entendem a qualidade de gastos como estratégica para o bom funcionamento da administração como um todo.

O critério de tomada de decisão de quem vence um processo de licitação no Brasil deve mudar de foco de ‘menor valor’ para ‘melhor valor’, ponderando outros critérios como qualidade dos serviços ou produtos a serem adquiridos. Segundo Motta (2010):

> Isso não significa desperdiçar o dinheiro público, e sim evitar a compra de um produto ruim, desperdiçando dinheiro do contribuinte.

## 2.14 MODELO DE CONTRATAÇÃO DE TI DA APF

Para definição do processo de Modelo de Contratação de TI da APF - MCTI, foi considerado o material de maior relevância disponível, que ilustra o que fazer, como fazer, quem deve fazer e quando fazer. O material é o Guia Prático para Contratação de Soluções de Tecnologia da Informação em sua versão 1.1 (SLTI, 2011).

Em 2011 foi divulgada a última versão do Guia Prático para Contratação de Soluções de TI da APF, que apresentou um esclarecimento maior do processo, com exemplos, *templates* e uma descrição das atividades. O Guia organiza papéis, responsabilidades e atividades que devem ser desempenhadas para uma contratação de TI, além de propor uma divisão de fases nas etapas de contratação. Apresenta também a relação de documentos que servirá de apoio para a contratação e para sua gestão e por fim, artefatos e modelos que irão compor o documento de Termo de Referência (TR), com o conteúdo a ser especificado na busca de maior aderência ao objetivo da contratação.

O TR consolida o estudo prévio da contratação e, segundo o art. 2 da IN04, é realizado pela equipe de planejamento da contratação e aprovação pela autoridade competente (Art. 17, §4º) de um determinado órgão público. Para a conclusão do estudo prévio que gera o TR, os gestores de TI devem confeccionar na fase de Planejamento da Contratação, os seguintes artefatos: DoD, Plano de Sustentação, Análise de Viabilidade, Estratégia da Contratação e Análise de Riscos. Com tal abrangência, a atividade de composição do TR, e o resultante conteúdo desse documento, terão substancial impacto nas demais fases do processo.

### 2.14.1 O Processo

O Guia possui uma versão da IN04, principal condutora dessa pesquisa e que foi resumida na Figura 2-8.

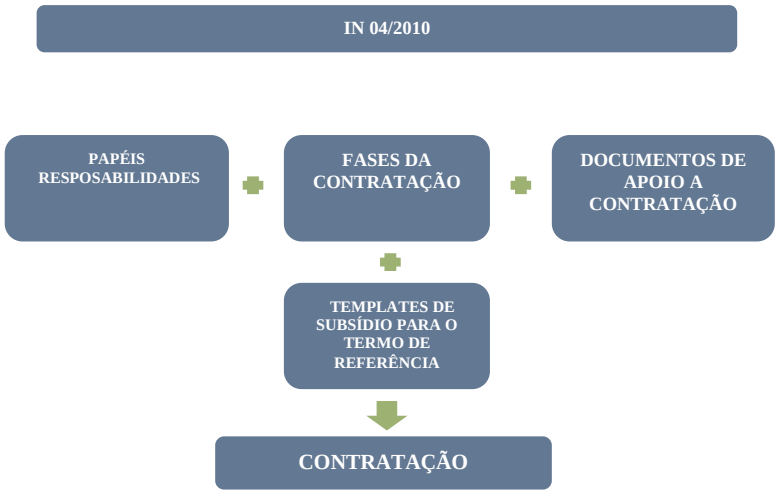


Figura 2-8 Ideia geral da IN04 (interpretação do autor).

A IN04 é a consolidação de um conjunto de boas práticas, com atores, fases, documentos e *templates* que subsidiam as contratações de TI da APF, e a SLTI entende que este conjunto

constitui um Modelo de Contratação de Soluções de TI (SLTI, 2011), cujo macroprocesso é apresentado na Figura 2-9. Por esse motivo, neste trabalho, essa referência foi utilizada para descrever o processo de contratação de TI da APF, considerando especificamente a versão da IN04/2010, que foi apresentada no Guia Prático para Contratação de Soluções de TI.

Para se iniciar uma contratação de TI e avaliar os seus riscos , presume-se que o gestor responsável pela contratação, tenha o conhecimento de que:

- Exista um instrumento de planejamento, denominado PPA - Plano Plurianual;
- Exista uma EGTI (Estratégia Geral de TI);
- Exista um PDTI (Plano Diretor de TI), originado do Planejamento da área de TI;
- Exista a demanda no PDTI ou em documento similar;
- Exista um recurso/programa de despesa especifico para a futura contratação;
- Exista uma formalização de alguma área demandante (DoD – Documento de Oficialização da Demanda) para que a TI possa especificar a contratação.

Com essas premissas, o modelo MCTI poderá ser aplicado na contratação. Sendo assim, segundo a IN04, em seu art. 8º, as contratações de TI devem seguir três fases:

- PCTI - Planejamento da Contratação;
- SFTI - Seleção do Fornecedor;
- GCTI - Gerenciamento do Contrato.

Para cada fase, existem processos, atividades, artefatos e atores. Para se ter uma dimensão da complexidade do processo, lista-se na Tabela 2-3 a quantidade de itens a serem considerados para uma contratação de TI estar aderente à IN04.

**Tabela 2-3** Distribuição dos processos, atividades, artefatos e atores do MCTI. (Adaptado de SLTI, 2011).

| Fases | Processos | Atividades | Artefatos | Atores |
|---|---|---|---|---|
| **PCTI** | 5 | 41 | 6 | 7 |
| **SFTI** | 3 | 7 | 1 | 4 |
| **GCTI** | 5 | 19 | 4 | 5 |

Ou seja, contratar uma solução de TI envolve responsabilidade, comprometimento, comunicação e predisposição em gerenciar riscos e orientação a resultado. A IN04 enfatiza que deve haver o trabalho conjunto entre as áreas. Uma área sozinha poderá iniciar o

trabalho de especificação da solução, mas com o envolvimento direto e participativo das áreas correlatas da contratação, para que seja prevista a maior quantidade possível de riscos e impactos da contratação em questão.

Quanto ao Macroprocesso do Modelo de Contratação de Soluções de TI de TI da APF, deve-se observar a Figura 2.9:

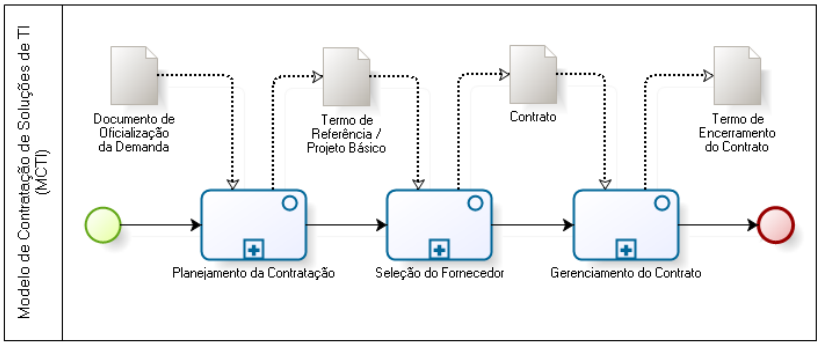


Figura 2-9 Modelo de contratação de solução de TI (MCTI), fases e produtos. (Fonte: SLTI, 2011).

A partir da formalização do DoD, que pode ser um memorando, uma ata de reunião, um e-mail ou mesmo uma conversa que pode ser registrada em formulário próprio do órgão, desde que indicado os requisitantes técnico, administrativo e demandante com a devida autorização superior, inicia-se o processo de contratação, desde que a demanda tenha sido prevista no PDTI do órgão. Existem algumas exceções que não serão motivo de desdobramento neste trabalho.

A área de TI deve especificar a solução juntamente com as demais áreas envolvidas no planejamento da contratação, realizando reuniões e alinhamentos necessários com todas as áreas envolvidas. Nessa fase, criam-se os artefatos e se elencam os riscos da contratação. Nesse momento, o gestor pode fazer bem o seu trabalho, procurando levantar o maior número de informações, ou simplesmente preencher o artefato para constar no processo. Um dos objetivos desse trabalho é evitar que os gestores negligenciem o documento de análise de riscos.

A análise de riscos encontra-se nessa fase de planejamento e o gestor deve mapear os riscos a serem gerenciados, e no próprio TR definir “gatilhos”, níveis de serviço e condições para a correta execução do contrato na fase de gerenciamento, evitando qualquer surpresa que impeça o adequado fornecimento dos bens e serviços, sob pena de multa e sanções diversas à licitante e em casos não previstos no edital, realizar a retenção do risco ou o compartilhamento, para diminuição do impacto.

Existem outros artefatos que compõem o processo de contratação como um todo, envolvendo o restante das fases de Planejamento, da Contratação, Seleção do Fornecedor e Gerenciamento do Contrato, tais como: Análise de Viabilidade, Plano de Sustentação, Estratégia da Contratação, Termos de Aceite e Compromisso, Termos de Entrega; que não serão objetos de detalhamento devido à limitação do escopo definida no início do trabalho, que é o artefato de analise de riscos da fase de Planejamento da Contratação. Entretanto, os artefatos listados foram aqui citados, para melhor definição do contexto do trabalho.

Realizado o preenchimento dos artefatos, as informações são consolidadas no termo de referência (TR). Este documento será encaminhado à área de licitações do órgão para que seja composto junto ao edital (em geral elaborado pela área de licitações). Essa etapa depende de aprovação da área jurídica e da própria área de licitações caso não encontrem nenhuma irregularidade no processo. O controle interno de cada organização também pode apoiar nessa fase. Esse documento é fundamental para o sucesso da contratação. Se mal elaborado, poderá gerar muitos problemas e uma gestão contratual ineficiente. Durante sua confecção, caso alguma característica desejada se verifique restrita a somente um ou a poucos fabricantes, a sua real necessidade deve ser reavaliada (NOTA TÉCNICA 02 SEFTI/TCU - 2008).

Para se escrever adequadamente um termo de referência de TI, além do disposto na IN04, deve-se seguir o roteiro da Nota Técnica 01 - SEFTI - TCU/2008. No TR devem ser considerados todos os fatores possíveis que possam comprometer o sucesso da contratação.

Uma vez concluído o Termo de Referência, inicia-se a fase de Seleção do Fornecedor. Esta fase é gerida pela área de licitações, mas a área de TI deve apoiar o pregoeiro e a equipe de apoio nas respostas dos questionamentos e a pedidos de impugnação do certame.

Realizado o pregão e definido um vencedor é designado um gestor do contrato, bem como fiscais para o contrato, onde o contrato será gerido com as métricas e parâmetros definidos no Edital/Termo de Referência.

### 2.14.2 Atores do MCTI

Uma lista de atores é descrita pelo processo, cada um com atividades específicas. Um ator pode executar vários papeis, o que reflete inclusive a realidade de parte do serviço público,

onde faltam servidores para exercer alguns papeis na área de TI. Abaixo, encontram-se os atores e uma breve descrição de suas atividades:

- Área Requisitante da Solução: Unidade ou órgão que irá demandar por meio do artefato DoD - Documento de oficialização da demanda, a contratação de uma solução de TI.
- Área de Tecnologia da Informação: Unidade do SISP responsável por gerir a TI de um órgão e designar os integrantes técnicos para contratações.
- Equipe de Planejamento da Contratação: Equipe composta por um integrante técnico (área de TI), um administrativo (área de contratos ou compras, por exemplo) e um requisitante (área demandante ou de negócio), para realizar principalmente o planejamento da contratação. Essa equipe realiza o preenchimento da Análise de Riscos, que surge nessa fase de planejamento da contratação. O principal documento de uma contratação a ser gerado pela equipe de Planejamento da Contratação é o Termo de Referência, documento que irá especificar o que se deseja comprar.
- Área de Licitações: Órgão ou setor responsável pelas atividades envolvidas no processo licitatório, e responsável pela fase SFTI, do modelo MCTI, com apoio da área de TI.
- Contratada: Entidade provedora da solução de TI que venceu o certame licitatório, representada pela figura do preposto.
- Gestor do Contrato: Servidor com atribuições gerenciais, técnicas e operacionais, relacionadas ao processo de gestão do contrato.
- Fiscal do contrato: Poderá existir um fiscal técnico, administrativo e requisitante, sendo que suas atribuições se diferenciam no aspecto de conteúdo.

Estes atores devem interagir constantemente na busca do alinhamento para a contratação.

### 2.14.3 A Fase de Planejamento da Contratação e seus Artefatos

O Planejamento da Contratação se inicia com o envio do Documento de Oficialização da Demanda - DOD à Área de Tecnologia da Informação, conforme mencionado anteriormente. Nessa etapa, chamada de iniciação do PCTI, é consolidado o DOD e instituída a equipe de Planejamento da Contratação.

O MCTI, desenhado no Guia Prático para Contratação de Soluções de TI, apresenta o seguinte sobre os artefatos da fase de planejamento da contratação:

Três processos são executados em paralelo: a Análise de Viabilidade da Contratação; o Plano de Sustentação e a Estratégia da contratação. A Análise de Riscos permeia todas as etapas do Planejamento da Contratação..

A Análise de Viabilidade tem como principal objetivo a verificação sobre se é viável ou não a continuidade do pedido de contratação.

O Plano de Sustentação tem a finalidade de garantir a continuidade do negócio enquanto este for necessário à APF.

A Estratégia da Contratação visa a definição de critérios técnicos, obrigações contratuais, responsabilidades e definições de como os recursos humanos e financeiros serão alocados para atingir o objetivo da contratação.

Paralelamente a tais atividades, na atividade de Análise de Riscos são identificados e analisados os riscos que podem comprometer o sucesso da contratação, bem como da execução contratual. Para cada risco, especificam-se os possíveis procedimentos de tratamento.

Exatamente nesse ponto, está a questão crucial de análise deste trabalho. O guia diz o que fazer, mas não como fazer. Com a criação do artefato, os gestores poderão ter um roteiro de como identificar os riscos, para depois tratá-los com a metodologia adequada.

Até por que, a IN04 obriga a execução da fase de Planejamento da Contratação, independente do tipo de contratação (IN04, art. 18.), o que inclusive é compatível com o dever institucional da Administração Pública de planejar.

A Figura 2-10 contextualiza a fase de Planejamento da Contratação e mostra a relevância que a Análise de Riscos tem neste processo.

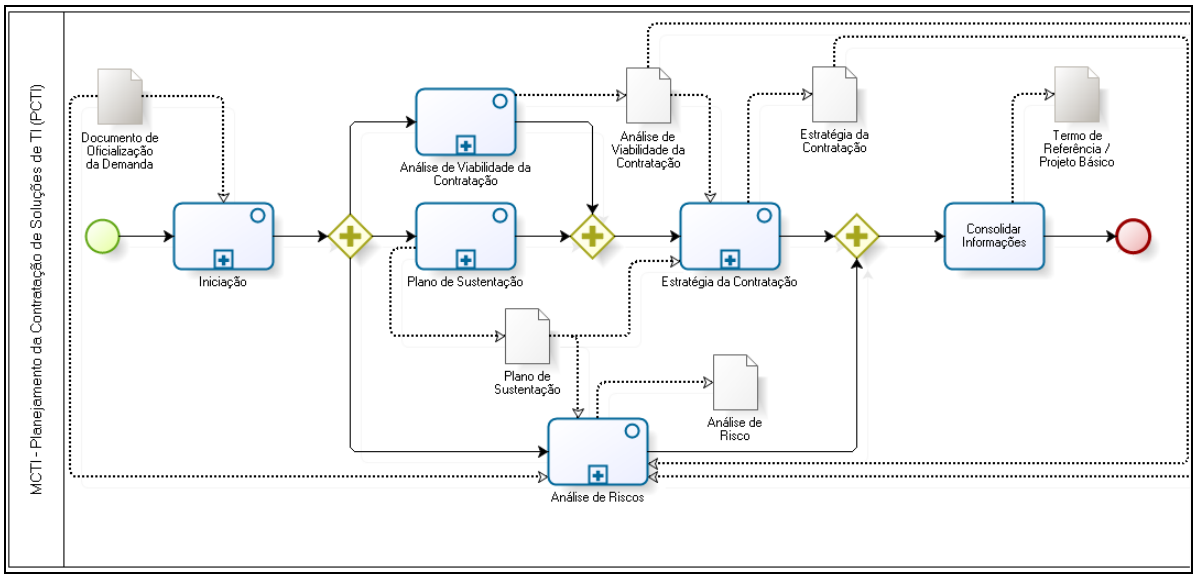


Figura 2-10 Fase de planejamento da contratação e o contexto da análise de riscos. (Fonte: SLTI, 2011).

Esse resumo do processo e dos artefatos permite agora um detalhamento melhor da análise de riscos e seus atores.

### 2.14.4 O Artefato de Análise de Riscos das Contratações de TI da APF

Um dos elementos que apoiam a atividade de planejamento da contratação é o artefato de Análise de Riscos cuja descrição é apresentada em SLTI (2011). O documento propõe o preenchimento do artefato de riscos sob duas perspectivas: da solução de TI e do processo de contratação de TI. O artefato resultante dessa atividade só pode ou só deve ser terminado após a conclusão dos outros artefatos, visto que, sendo estes artefatos considerados insumos para a Análise de Riscos, caso estejam incipientes ou incompletos implicarão numa Análise de Riscos também incipiente. A Figura 2-11.apresenta o artefato de Análise de Riscos.

| Risco | Risco | | | |
|---|---|---|---|---|
| | Probabilidade | Id | Dano | Impacto |
| | | 1 | | |
| | | … | | |

| Id | Ação Preventiva | Responsável |
|---|---|---|
| 1 | | |
| … | | |

| Id | Ação de Contingência | Responsável |
|---|---|---|
| 1 | | |
| … | | |

Figura 2-11 *Template* de análise de riscos. (Adaptado de SLTI, 2011).

O modelo considera para os atributos do *template* as seguintes afirmativas:

- **Risco**: Identificação dos riscos que podem comprometer o processo de contratação, resultando em atrasos ou em comprometimento da contratação.
- **Probabilidade**: Para cada risco, definir um percentual que representa a probabilidade de ocorrência do evento relacionado ao risco identificado.
- **Dano**: Para cada risco, definir os danos potenciais que o mesmo pode gerar no processo de contratação.
- **Impacto**: Para cada dano, descrever o impacto que o mesmo pode causar no processo de contratação.
- **Ação Preventiva**: Para cada risco, definir as ações a serem executadas para evitar a ocorrência do evento relacionado ao risco identificado.

- **Ação de Contingência**: Para cada risco, definir as ações que devem ser tomadas para remediar o impacto da ocorrência do evento relacionado ao risco identificado.
- **Responsável**: Para cada ação, identificar o responsável pela execução da ação relacionada. Neste momento, o responsável é um papel, área, setor e não necessariamente pessoas.

Além dos conceitos acima, o Guia recomenda que se sigam as seguintes orientações para preenchimento da Análise de Riscos:

1. Identificação dos principais riscos que possam comprometer o sucesso dos processos de contratação e de gestão contratual;
2. 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. Mensuração das probabilidades de ocorrência e dos danos potenciais relacionados a cada risco identificado;
4. Definição das ações previstas a serem tomadas para reduzir ou eliminar as chances de ocorrência dos eventos relacionadas a cada risco;
5. Definição das ações de contingência a serem tomadas caso os eventos correspondentes aos riscos se concretizem;
6. Definição dos responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência;
7. A análise de riscos permeia todas as etapas da fase de Planejamento da Contratação e será consolidada no documento final Análise de Riscos e
8. A Análise de Riscos será aprovada e assinada pela Equipe de Planejamento da Contratação.

As atividades enumeradas acima se encontram desenhadas na Figura 2-12, que detalha o processo de Análise de Riscos do Guia de Contratação de Soluções de TI.

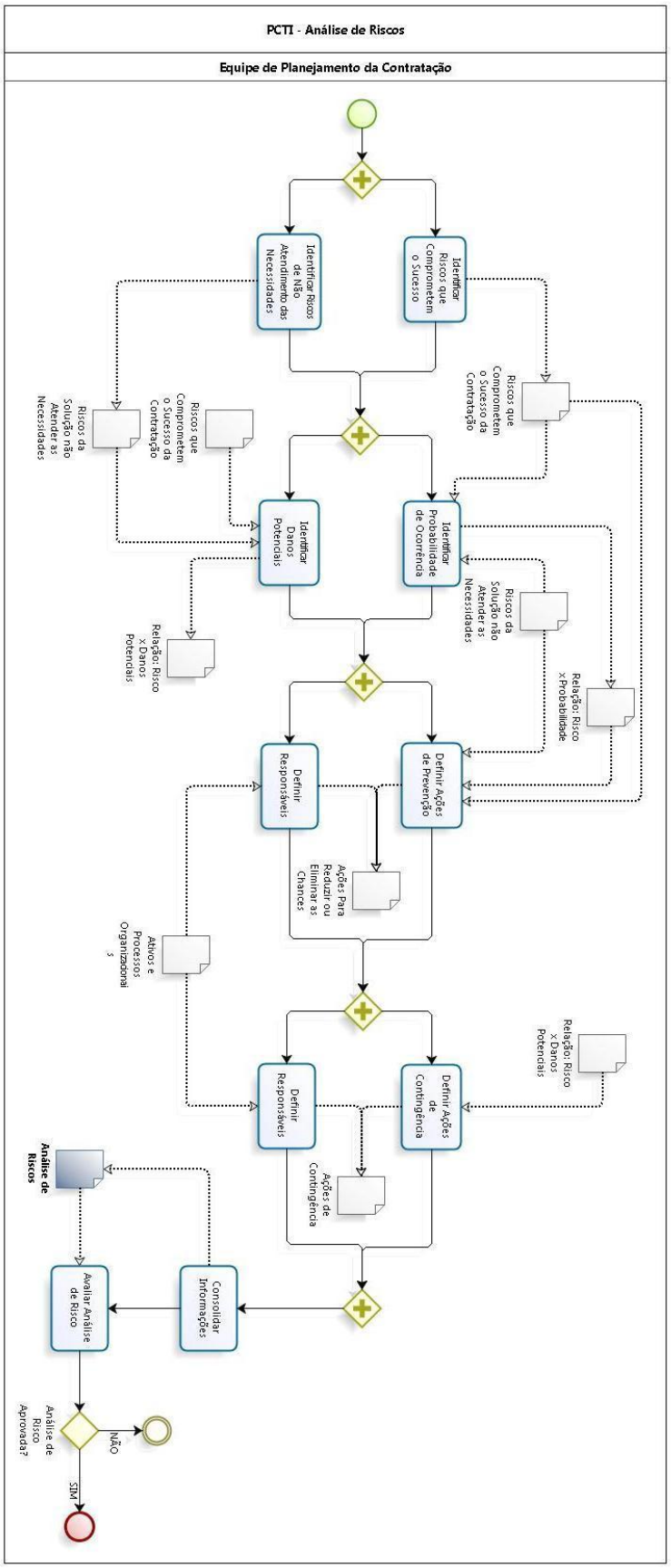


Figura 2-12 Subprocesso de Análise de Riscos. (Fonte: SLTI, 2011).

Nessa situação, a identificação dos riscos do processo de contratação de TI fica na dependência do talento ou experiência da equipe, sem uma contribuição do método de trabalho.

Ainda que a Análise de Riscos deva permear todas as etapas do planejamento da contratação (SLTI, 2011), implicando na necessidade de observar todo o processo de contratação para se identificar riscos, não se encontra no Guia, ou em fonte externa por ele apontada, a forma de se identificar as ameaças, vulnerabilidades, ativos, impactos e soluções envolvidas na fase de Identificação de Riscos. Por outro lado, há interesse em dotar o processo de um roteiro mínimo de como abordar a Identificação de Riscos no conjunto do processo, que se constitua como uma referência para os gestores de TI e assim defina um padrão básico de trabalho para utilização em diferentes contratações, o que permitiria a reutilização de artefatos, a comparação entre contratos, o aumento da maturidade dos processos, etc.

A criação do Guia que trata da Análise de Riscos nas contratações de TI direcionada aos órgãos que operacionalizam o processo foi de fato um passo importante, definindo um patamar a partir do qual se pode introduzir um detalhamento maior para Identificação de Riscos, inserindo-se a GR nessa atividade, tal como proposto neste trabalho, como contribuição para evolução do processo atual.

### 2.14.5 Análise do modelo atual quanto aos aspectos positivos

É importante destacar que anterior a essa proposta, inexistia um modelo de referência que de fato considerasse a GR e suas implicações para o aumento da maturidade dos processos. Dessa forma, o simples fato de já se ter um modelo de referência, é um ponto positivo, pois partiu de uma maturidade inexistente para um modelo a ser preenchido. Os demais aspectos observados foram os seguintes:

a) O modelo apresentado é dividido em duas classificações, que são respectivamente "Riscos do Processo de Contratação (riscos do processo)" e "Riscos da Solução de Tecnologia da Informação (riscos do produto/serviço)". Ou seja, permite a classificação dos riscos em dois níveis de abordagem: Processo x Tecnologia, permitindo ao gestor levantar as informações com as pessoas habilitadas a falar (cada uma do assunto de seu maior conhecimento).
b) O modelo considera suficiente para fins do tratamento do risco levantado a

verificação da Probabilidade x Dano x Impacto x Ação Preventiva e Ação de contingência, bem como um responsável. Isso torna o modelo bastante objetivo e relativamente simples de se preencher, sob o aspecto da análise de riscos.

c) O modelo não limita a identificação de riscos e permite a descrição de quantos riscos forem necessários até que se encontre uma margem mínima.
d) O modelo atribui responsabilidades, o que é fundamental para iniciar e monitorar as atividades de gestão de riscos.
e) O modelo segue a referência da ABNT NBR ISO 31010 por utilizar uma de suas metodologias de tratamento de riscos (matriz probabilidade x impacto). Por isso está alinhado com essa norma.

### 2.14.6 Análise do modelo atual quanto aos aspectos a serem evoluídos

A seguir os aspectos analisados:

- Não é exemplificativo.

Não existe nenhuma referência ou fonte indicativa, que os gestores possam consultar, para entender qual é o conceito de riscos, impacto, probabilidade, etc. Alguns podem consultar fontes oficiais, outros, entretanto poderiam simplesmente escrever a primeira palavra que vier na memória, mas este pode não ser a que identifica o risco por completo.

- É ambíguo, pode ter várias interpretações.

Como não é um documento explicativo, infere-se que cada um possa interpretar de um jeito e preencher da sua maneira, gerando contratações do mesmo produto, em órgãos diferentes, com levantamento de riscos completamente distintos. Pode acontecer, inclusive, de uma mesma empresa ter que prestar o mesmo serviço em órgãos diferentes, mas um contrato sendo mais rigoroso que o outro, ou mais bem especificado que o outro. Isso poderá permitir melhores resultados em um órgão, se comparado a outro.

- Não é obrigatório.

Alguns compradores públicos podem não preencher os artefatos de planejamento da contratação e consequentemente ignorar os documentos de análise de riscos, gerando direto o TR. Outros, sabendo da vulnerabilidade do documento, apenas assinam e colocam um risco qualquer, fazendo que este documento seja apenas *"pro forma*".

- Não considera se quem preenche é a pessoa apta para aquela atividade.

Muitas pessoas são designadas para exercer certas atividades por força do poder de delegação de seus superiores, que podem não estar considerando aspectos objetivos e de competência, para indicar as pessoas para tal responsabilidade. O processo de definição das pessoas que irão fazer este trabalho envolve sensibilização, conhecimento, dedicação e compromisso sobre o assunto. Assim, não é suficiente indicar nomes; essas pessoas devem ser preparadas e treinadas.

- Não garante que os principais pontos da contratação serão considerados.

Apesar de o documento de análise de riscos ser uma continuidade e uma revisão dos outros artefatos, tais como Análise de Viabilidade, Plano de Sustentação e Estratégia da Contratação, nada garante que os gestores revisem todos os artefatos para elencar os riscos da contratação. Não porque não querem, mas porque isso não está explicado ou por não terem um instrumento facilitador.

- Não é revisado.

Realizado o planejamento da contratação e o preenchimento da análise de risco, esse documento geralmente fica arquivado e não é revisado durante o ciclo de vida da contratação.

- Não é um documento tão público quanto deveria.

Os artefatos da contratação não são comumente disponibilizados nos sítios dos órgãos públicos, o que impede o cidadão de entender como foi elaborado o edital em questão.

- Não considera classificações essenciais, como pessoas, atividades, papéis e responsabilidades da contratação como um todo.

O modelo não leva em consideração as variáveis citadas nos documentos preliminares. Ele apenas pede que se listem os riscos. Se o gestor esquecer-se de alguma variável, ela ficará exposta. Apesar de ser intuitivo fazer do documento de análise de riscos uma continuidade dos artefatos, isso dependerá única e exclusivamente do interesse do gestor responsável.

- Não gera uma base de conhecimento.

Uma vez listados os riscos, eles são impressos e inseridos no processo. Mas ficam arquivados, sem atualizações, geralmente nos computadores de quem gerou o artefato. O conhecimento adquirido não é replicado, incrementado ou reutilizado para outras áreas ou para outros órgãos, sequer na contratação em questão.

- Não é automatizado para melhoria de próximas contratações.

Existem iniciativas de automação do Modelo de Contratações de TI do governo brasileiro, mas que até agora não foram implementadas.

- Não considera riscos com relação a problemas de comunicação.

Na prática, a falta de comunicação, pouca comunicação ou mesmo a comunicação com entendimentos errados, leva a percepções de que pode estar tudo bem com a contratação. A análise de riscos é um processo de planejamento que precisa de várias interações para ficar maduro e deve ser transparente principalmente quanto à comunicação.

- Não considera riscos políticos, que são críticos nos cenários das organizações públicas.

Muitas vezes gestores de TI são pessoas com habilidades e cargos que conseguem gerenciar um contrato com relativa segurança. Entretanto fatores políticos podem prevalecer sobre questões técnicas em determinadas situações, que não serão objeto de detalhamento.

- GR deveria ser inclusiva

O conceito e o processo de riscos descritos na IN04 não são colaborativos muito menos inclusivos. Cada gestor segue seu caminho, faz sua contratação e depois é auditado pelo mesmo Tribunal. Seria interessante alinhar a IN04 e tornar suas atividades inclusivas, facilitando a comunicação e as demandas dos órgãos de controle perante os órgãos que contratam.

Diante do exposto e, com base nos parâmetros apontados, a seguir será proposta na Figura 2-13 uma atualização do processo de Identificação de Riscos, com o uso da ferramenta de modelagem de Processos - *Bizagi Process Modeler*.

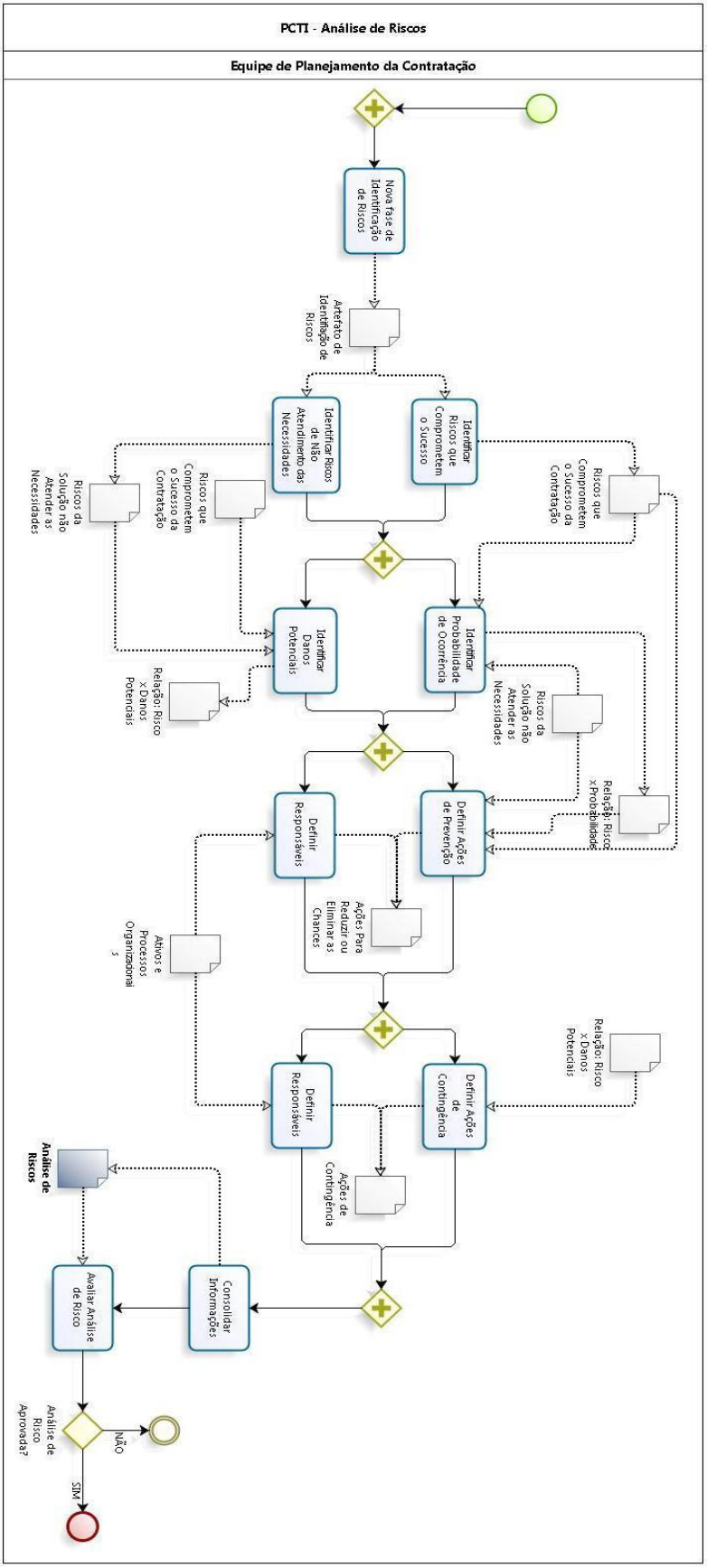


Figura 2-13 Subprocesso de Análise de Riscos atualizado com o novo artefato

Com esse processo adequado, a atividade de identificação de riscos, que está contida no artefato Análise de Riscos da IN04, estaria com sua importância em evidência, o que trará maior detalhamento das atividades de identificação de riscos e assim permitiria um detalhamento maior dos riscos identificados.

Após a contribuição ao modelo de Analise de Riscos, serão estudadas a seguir as referências para o termo “risco”, que possui diversos significados e necessita ser explorado e mais bem compreendido para o contexto deste trabalho. No capítulo seguinte, o artefato proposto será desenhado.

# 3. REVISÃO DE LITERATURA - RISCOS

Atualmente, a TI aparece como um dos principais agentes de risco nas organizações (DE HAES E VAN GREMBERGEN, 2004) e a maneira com que os investimentos e as tecnologias têm sido governados têm refletido na satisfação dos executivos das organizações (PETERSON, 2004).

Nas organizações públicas esse cenário não é muito diferente. Adquirir TI somente não basta, é preciso governá-la. Afinal, uma aquisição pelo menor preço de vários computadores, por exemplo, que não possuem gestão de suas garantias e que fiquem armazenados em locais impróprios, poderá neutralizar todos os benefícios de uma contratação. Essas ações, também constituem riscos que devem ser previstos e refletem na insatisfação dos executivos, caso não sejam devidamente elencadas e tratadas pela área de TI.

Nesse contexto, a governança de TI se transforma numa tentativa de garantir que o dinheiro investido em TI esteja agregando valor à organização e diminuindo assim os riscos (DE HAES & VAN GREMBERGEN, 2004).

Empresas que possuem modelos de governança de TI geralmente apresentam resultados superiores aos de seus concorrentes, principalmente porque tomam as decisões de TI mais seguras, evitando riscos de tomada de decisão (WEILL e ROSS, 2004; WEILL e ROSS, 2004a).

Sendo assim, as ideias expostas podem influenciar diretamente na governança de TI, pois apesar de saberem da relevância, executivos que não priorizam a TI, podem ter resultados inferiores aos de seus concorrentes, ficando com um percentual menor de participação no mercado em relação à concorrência. E para se ter tecnologia, precisa-se de serviços, ativos, equipamentos, além de mão de obra. Tudo isso envolve contratações, e, gerenciar os riscos dessa etapa envolve diversas variáveis.

É preciso ter cuidado ao especificar as soluções de TI e observar as questões sobre um aspecto de 360º da organização. É fundamental que membros com mais tempo de trabalho e experiência, principalmente nas organizações públicas que lidam com dinheiro do contribuinte, estejam disponíveis para opinar e elencar as possibilidades e impactos em

toda a organização, no que diz respeito à contratação de TI, principalmente quando se trata de uma aquisição de grande valor.

Obviamente essa estrutura de verificação para processos menores pode ser resumida, mas de fato é necessário  um modelo direcionador para se identificar riscos das contratações com critérios mínimos.

## 3.1 RISCOS - CONCEITOS

Após grandes escândalos corporativos como os casos das empresas Xerox, Enron, World.com por volta de 2002, as organizações perceberam a importância de práticas institucionais que enfatizem a transparência e a ética, criando a demanda por boas práticas de governança do mundo inteiro, em busca da diminuição de riscos em diversos sentidos. Esse marco, trouxe a implementação de controles internos, com a utilização da SOX - *Sarbanes Oxly* (SILVA, *et al*, 2009).

Foi nesse período que o assunto "risco" foi tratado com mais atenção pelas organizações. O tema é amplo e possui diversas origens no mundo. Em função da existência de várias fontes de informação é possível que a GR possua definições ambíguas.

Segundo a ABNT NBR ISO 31000, o conceito de riscos pode assim ser definido:

> Organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de risco.

Para Gimenes (2003), identificar os riscos pode não ser uma tarefa simples, pois, as ameaças e incertezas que podem gerar prejuízos às organizações são muito mais abrangentes do que se poderia imaginar à primeira vista.

De Cicco (1985) considera que o risco é uma combinação da probabilidade de ocorrência e das consequências de um evento perigoso especificado (acidente ou incidente). Segundo o autor, existem dois elementos básicos: 1) a probabilidade de um perigo ocorrer e 2) as consequências de um evento perigoso.

A palavra risco, segundo Bernstein (1996), tem origem no italiano antigo *risicare* cujo significado é ousar, levando à conclusão de que o risco é uma escolha e não um destino. Portanto, se o risco é uma opção, envolvendo uma tomada de decisão, essa decisão, que

possui consequências importantíssimas para o futuro das instituições, deve ser baseada em critérios coerentes e mensuráveis (EMBLEMSVAG, 2002).

Bernstein (1996) afirma ainda que a capacidade de definir o que poderá acontecer no futuro e de optar entre várias alternativas é importante às organizações e que essa capacidade de administrar o risco e de fazer opções ousadas e de inovar é que formam elementos chaves da energia que impulsionam o sistema econômico.

Marshall (2002) recomenda distinguir o termo risco de incerteza. Para o autor, risco é algo já experimentado, apresentando base histórica de informações e aceito por antecipação ao processo de investimento, constituindo-se assim numa ação consciente. Já a incerteza refere-se à imprevisibilidade de um fenômeno por total desconhecimento do mesmo.

Marshall (2002) ainda ressalva que risco se aplica a resultados que, embora não certos, tenham probabilidades que possam ser estimadas pela experiência ou por dados estatísticos e a incerteza está presente quando o resultado não pode ser previsto, nem mesmo em um sentido probabilístico.

Processos de gestão de riscos utilizam informações de fontes variadas como dados sobre ativos e suas vulnerabilidades, registros de sistemas, decisões gerenciais, dentre outros. Desta forma, recursos que possam auxiliar na manipulação de informações deste complexo arcabouço constituem necessidades reais e relevantes a serem consideradas (GUALBERTO, 2011).

Diversos autores têm escrito sobre a classificação dos riscos, como é o caso de Hamilton (2000) que identifica seis tipos de riscos a que as organizações estão sujeitas: estratégicos, financeiros, operacionais, comerciais, técnicos e ambientais. Segundo o mesmo autor, muitos deles são pequenos e provocam baixos impactos nos negócios, entretanto, alguns são grandes o suficiente para provocar enormes perdas e até a falência da organização.

Na gestão da TI, a preocupação com os riscos é um aspecto chave, uma vez que assegura que os objetivos estratégicos do negócio não são colocados em risco por falhas da TI. Os riscos associados a problemas de tecnologia são cada vez mais evidentes nas agendas dos administradores, dado que o impacto no negócio desse tipo de falha pode ter sérias consequências, principalmente em se tratando de organizações com elevada dependência estratégica em relação à TI.

Nesse sentido, a análise de risco tem se tornado uma área de importância na economia atual, pois a maioria das decisões econômicas é tomada em cenários que envolvem incerteza. As fontes de incerteza são múltiplas e extensivas, abrangendo riscos associados a mercados, fornecedores, meteorologia, tecnologia, dentre outros (CHAVAS, 2004).

Cruz; Andrade; Figueiredo (2011) propõem que riscos sejam identificados em todos os momentos do procedimento licitatório a ser executado e para cada um deles, sejam também identificados os riscos de obstáculo à boa consecução da licitação. Sugerem também que se realizem algumas etapas para se minimizar riscos, dentre elas:

- Histórico de eventos danosos em licitações;
- Levantamento dos riscos da licitação;
- Histórico de eventos danosos em contratações;
- Levantamento dos riscos na execução contratual;
- Plano de ação para tratamento de riscos;
- Plano de ação para continuidade de negócio;
- Impactos dos riscos;
- Relatórios dos riscos.

Em síntese, existem vários conceitos sobre o tema e uma gama de pluralidade dos entendimentos. No Brasil, a terminologia de riscos foi traduzida e adaptada com a ABNT NBR ISO GUIA 73 de 2009 (ABNT, 2008b). Uma segunda Norma ABNT, a NBR ISO 31000 de 2009 harmonizou os processos e atividades da GR (ABNT, 2009a) e uma terceira, aborda as metodologias para tratamento de riscos (ABNT, 2012).

Para diminuir as inferências sobre os vários conceitos de riscos existentes, será proposta no capítulo seguinte uma harmonização terminológica no artefato que será criado para diminuição das ambiguidades que possam vir a causar dúvidas, especificamente no modelo de Análise de Riscos da IN04.

Após a introdução dos conceitos por autores que versaram sobre o tema serão apresentados os relacionamentos do assunto com itens de contratação e governança de TI, além das normas de GR, juntamente com seus principais conceitos e parâmetros a serem considerados para a melhoria do modelo de Análise de Riscos da contratação da APF.

## 3.2 COBIT 4.1 - VISÃO SOBRE RISCOS

O COBIT *(Control Objectives for Information and Related Technologies)* foi desenvolvido pelo *IT* (*Governance Institute)* como um guia das melhores práticas para a governança de TI. Trata-se de um modelo desenvolvido para alinhar os recursos e processos de TI com os objetivos do negócio, padrões de qualidade, controle monetário e necessidades de segurança (ITGI, 2007).

O COBIT 4.1 destaca-se pela sua grande aceitação em todo o mundo, o que possibilita uma linguagem comum de amplo entendimento entre os envolvidos com a governança de TI (ITGI, 2007).

Ele fornece um modelo padrão de referência e linguagem que permite distinguir e gerenciar as atividades que competem à TI. O modelo possui 4 domínios inter-relacionados aos requisitos de informações e recursos de TI: (i) domínio de planejamento e organizações (PO); (ii) domínio aquisição e implementação (AI); (iii) domínio entrega e suporte (DS); e (iv) domínio de monitoração e avaliação (ME), (ITGI, 2007).

A Figura 3-1 ilustra os domínios de atuação do COBIT 4.1:


Figura 3-1 Áreas de foco do COBIT 4.1 na governança de TI, incluindo a GR. (Fonte: ITGI, 2007).

Para esta pesquisa será considerada a visão do processo PO9 - Avaliar e gerenciar os riscos de TI. A seguir é apresentado na Figura 3-2 o contexto deste processo.

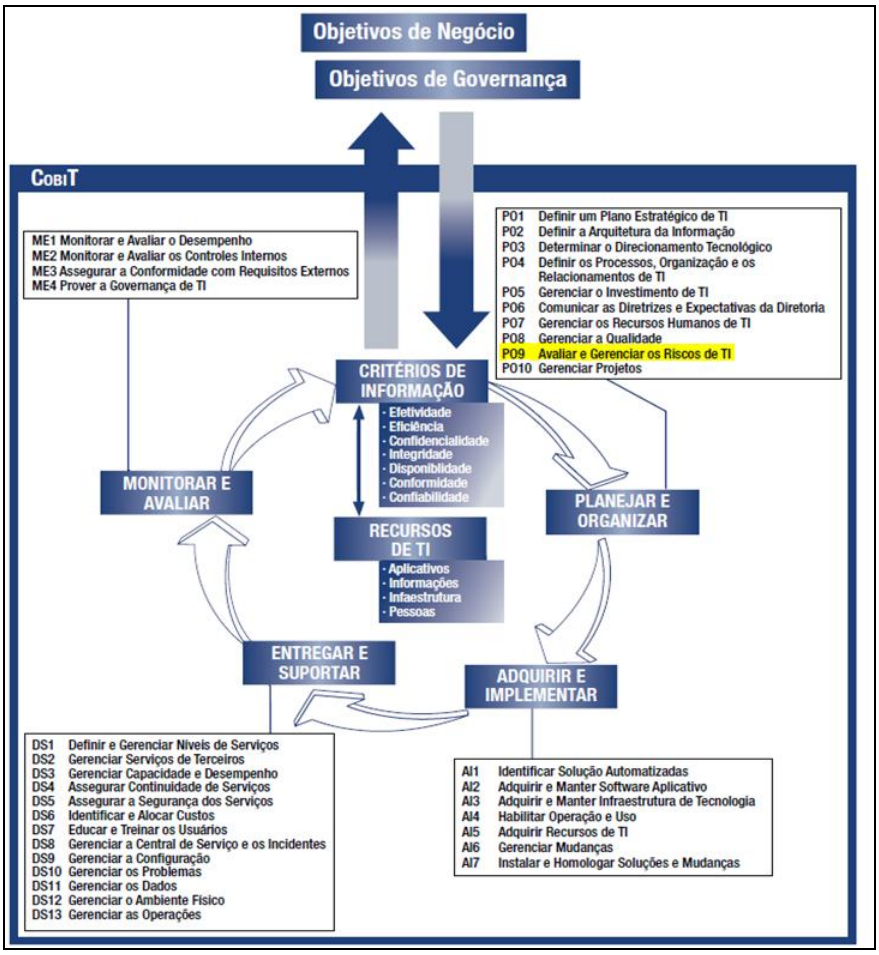


Figura 3-2 Visão geral do COBIT e o contexto do processo PO9. (Fonte: ITGI, 2007).

### 3.2.1 Processo PO9 - Avaliar e gerenciar os riscos de TI

O processo apresenta a preocupação que os funcionários mais experientes da corporação devem ter com o risco, e uma ideia clara do apetite de risco da empresa. Esses profissionais devem ficar atentos aos requerimentos de conformidade e transparência sobre os riscos da organização (ITGI, 2007).

O *framework* COBIT 4.1 sugere que se crie e mantenha uma estrutura de GR, o que não é percebido explicitamente no modelo atual de contratações do MP. Qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado, consequentemente mantido, e o processo atual não sugere a revisão dos riscos durante as fases seguintes.

Estratégias de mitigação de risco devem ser adotadas para minimizar o risco residual a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas e expresso em termos financeiros para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis. O PO9 - Avaliar e Gerenciar os Riscos de TI é o processo

do COBIT que pode contribuir para melhoria do modelo de Análise de Riscos da contratação brasileiro, por possuir recomendações muito utilizadas por diversas organizações. A seguir, será detalhado o que sugere cada subprocesso, segundo o COBIT 4.1.

#### 3.2.1.1 PO9.1 Alinhamento da GR e de negócios

Estabelecer uma estrutura de GR de TI alinhada com a estrutura de GR da corporação.

#### 3.2.1.2 PO9.2 Estabelecimento do contexto de risco

Estabelecer o contexto com a definição dos contextos interno e externo de cada avaliação de risco, o objetivo da avaliação e os critérios pelos quais os riscos são avaliados.

#### 3.2.1.3 PO9.3 Identificação de eventos

Identificar eventos que podem impactar negativamente nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação. Registrar e manter um histórico dos riscos relevantes.

#### 3.2.1.4 PO9.4 Avaliação de risco

Avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos.

A probabilidade e o impacto associado ao risco inerente e residual devem ser determinados individualmente, por categoria e com base no portfólio da organização.

#### 3.2.1.5 PO9.5 Resposta ao risco

Desenvolver e manter um processo de respostas a riscos para assegurar que controles com uma adequada relação custo-benefício mitiguem a exposição aos riscos de forma contínua. O processo de resposta ao risco deve identificar estratégias de risco, tais como evitar, reduzir, compartilhar ou aceitar o risco, determinar responsabilidades, e considerar os níveis de tolerância definidos.

#### 3.2.1.6 PO9.6 Manutenção e monitoramento do plano de ação de risco

Priorizar e planejar as atividades de controle em todos os níveis da organização para implementar respostas aos riscos identificados, incluindo a identificação de custos x benefícios e responsabilidade pela execução. Obter aprovações para ações recomendadas e aceitação de quaisquer riscos residuais e assegurar que as ações aprovadas sejam assumidas pelos donos dos processos afetados. Monitorar a execução dos planos e reportar qualquer desvio para a alta direção. A Tabela 3-1 indica os papéis e funções sobre as atividades de risco, por meio de uma tabela RACI (Responsável/Responsabilizado/Consultado/Informado).

**Tabela 3-1** Papéis e funções sobre as atividades de riscos - Tabela RACI. Fonte: ITGI, 2007.

| Tabela RACI / Atividades | CEO | CFO | Executivo de Negócio | CIO | Proprietário do Processo de Negócio | Responsável por Operações | Responsável por Arquitetura | Responsável por Desenvolvimento | Responsável pela Administração de TI | PMO | Conformidade, auditoria, risco e segurança |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Promover o alinhamento da gestão de riscos (por exemplo: avaliação de riscos); | A | R/A | C | C | R/A | I | | | | | I |
| Entender os objetivos estratégicos de negócio relevantes; | | C | C | R/A | C | C | | | | | I |
| Entender os objetivos de processos de negócio relevantes; | | | | C | C | R/A | | | | | I |
| Identificar objetivos internos de TI e estabelecer contexto de risco; | | | | | R/A | | C | C | C | | I |
| Identificar eventos associados com objetivos [alguns eventos são orientados ao negócio (negócio é A); alguns são orientados a TI (TI é A, negócio é C)]; | I | | | A/C | A | R | R | R | R | | C |
| Avaliar criticamente os riscos associados com eventos; | | | | A/C | A | R | R | R | R | | C |
| Avaliar respostas aos eventos; | I | I | A | A/C | A | R | R | R | R | | C |
| Planejar e priorizar as atividades de controle; | C | C | A | A | R | R | C | C | C | | C |
| Aprovar e assegurar o financiamento de planos de ações para riscos; | | A | A | | R | I | I | I | I | | I |
| Manter e monitorar os planos de ações para riscos | A | C | I | R | R | C | C | C | C | C | R |

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Com essa tabela, podem-se definir os papéis que devem ser comunicados no processo de GR, segundo o COBIT 4.1.

### 3.2.2 Níveis de maturidade COBIT 4.1

Além da definição de papéis, o COBIT 4.1 define ainda níveis de maturidade para riscos. As informações a seguir foram extraídas integralmente do COBIT 4.1.

#### 3.2.2.1 Inexistente - nível zero

Quando não acontece avaliação de risco para processos e decisões de negócio. A organização não considera os impactos no negócio associados a vulnerabilidades da segurança e incertezas de projetos de desenvolvimento. Gerenciar riscos não é considerado relevante para adquirir soluções ou entregar serviços de TI.

#### 3.2.2.2 Inicial/*ad hoc* - nível um

Quando os riscos de TI são considerados de forma *ad hoc*. Avaliações informais de risco de projeto são realizadas quando solicitadas em cada projeto. Avaliações de risco são às vezes identificadas em um plano de projeto, mas raramente atribuídas aos gerentes correspondentes.

Riscos específicos relacionados a TI, como segurança, disponibilidade e integridade, são ocasionalmente considerados nos projetos. Os riscos de TI que afetam o dia-a-dia da operação são raramente discutidos em reuniões gerenciais. Mesmo onde os riscos são levantados, as ações para mitigá-los são inconsistentes. Está surgindo um entendimento de que os riscos de TI são importantes e devem ser considerados.

#### 3.2.2.3 Repetível, porém intuitivo - nível dois

Quando existe uma abordagem imatura e inicial de avaliação de risco utilizada a critério de alguns gerentes de projeto. A gestão de risco é superficial e geralmente aplicada somente a grandes projetos ou em resposta a problemas. O processo de mitigação de risco está começando a ser implementado onde são identificados riscos.

#### 3.2.2.4 Processo definido - nível três

Quando uma política corporativa de gestão de risco define onde e como conduzir as avaliações de risco. A gestão de risco segue um processo definido e documentado. Há treinamento em gestão de risco disponível para todo o pessoal. Decisões de seguir o processo de gestão de risco e receber treinamento são deixadas a critério de cada indivíduo. A metodologia de avaliação de risco é convincente, robusta e assegura a identificação dos riscos-chave para o negócio. Um processo para mitigar os riscos-chave é implementado após a identificação dos riscos. As responsabilidades pela GR estão definidas nas descrições de cargo.

#### 3.2.2.5 Gerenciado e mensurável - nível quatro

Quando a avaliação e a gestão de risco são procedimentos padronizados. As exceções do processo de gestão de risco são relatadas à Diretoria de TI. A gestão de risco de TI é uma responsabilidade da Alta Direção. O risco é avaliado e mitigado no nível de projeto e também regularmente no nível de operação de TI. O comitê executivo é avisado das mudanças no ambiente de negócios e de TI que podem afetar consideravelmente os

cenários de riscos relacionados à TI. A Diretoria é capaz de monitorar a posição do risco e tomar decisões fundamentadas no nível de exposição aceitável. Todos os riscos identificados têm um responsável definido, e o comitê executivo e a diretoria de TI estabeleceram os níveis de risco que a organização irá tolerar. A área de TI desenvolveu indicadores padrão para avaliar riscos e definir taxas de riscos/retornos. A área de TI aloca recursos para um projeto de gestão de risco operacional a fim de reavaliar periodicamente os riscos. Um banco de dados de gestão de risco é estabelecido, e uma parte dos processos de gerenciamento de risco está começando a ser automatizada. A área de TI estuda estratégias de mitigação de riscos.

#### 3.2.2.6 Otimizado - nível cinco

Quando o gerenciamento de risco atingiu um estágio de desenvolvimento em que há um processo organizacional estruturado em vigor e bem gerenciado. Boas práticas são aplicadas em toda a organização. A captura, a análise e o relato de dados de gestão de risco estão altamente automatizados. É recebida orientação de lideranças da área, e a organização de TI participa de grupos de discussão para troca de experiências. A gestão de risco está totalmente integrada às operações de negócio e de TI, é bem aceita e envolve extensivamente os usuários dos serviços de TI. A Direção de TI detecta e age quando grandes decisões operacionais e de investimentos de TI são tomadas sem considerar o plano de gestão de risco. A direção de TI avalia continuamente as estratégias de mitigação de risco.

## 3.3 PMBOK – VISÃO SOBRE RISCOS

O *Project Management Body of Knowledge* (PMBOK) foi elaborado pelo *Project Management Institute* (PMI), uma organização não governamental dedicada às necessidades dos gerentes de projetos do mundo todo. O PMBOK é um *framework* genérico, destinado ao gerenciamento de projetos para todas as áreas do conhecimento. Ele foi elaborado com a colaboração de várias dezenas de profissionais afiliados ao PMI e de origens diversas. A primeira versão do PMBOK foi publicada em 1996 (FERNANDES; ABREU, 2006).

O PMBOK formaliza diversos conceitos em gerenciamento de projetos, como a própria definição de projeto e do seu ciclo de vida. O principal objetivo do PMBOK é identificar um conjunto de conhecimentos sobre gerenciamento de projetos reconhecido como boa

prática. Estes conhecimentos estão categorizados em nove áreas e os processos relacionados são organizados em cinco grupos de processos ao longo do ciclo de vida do projeto (PMI, 2004).

As áreas de conhecimento caracterizam os principais aspectos envolvidos em um projeto e no seu gerenciamento: (i) Integração, (ii) Escopo, (iii) Tempo, (iv) Custos, (v) Qualidade, (vi) Recursos humanos, (vii) Comunicações, (viii) Riscos e (ix) Aquisições. Os cinco grupos de processos de gerenciamento de projetos são: (i) Iniciação, (ii) Planejamento, (iii) Execução, (iv) Monitoramento e Controle, e (v) Encerramento (PMI, 2004).

Para o PMBOK, em sua área de conhecimento sobre riscos, é definido que risco do projeto é um evento ou condição incerta que, se ocorrer, terá um impacto positivo ou negativo sobre pelo menos um objetivo do projeto, como escopo, tempo, custo ou qualidade. Um risco poderá ter uma ou mais causas, e se ocorrer, um ou mais impactos, além de eventos (PMI, 2004, p. 238).

O gerenciamento de riscos do projeto inclui os processos de planejamento do gerenciamento de riscos, identificação dos riscos, análise qualitativa dos riscos, análise quantitativa dos riscos, planejamento de respostas a riscos e monitoramento e controle dos riscos. A maioria desses processos é atualizada durante todo o projeto e interagem entre si, além de outros processos de outras áreas do conhecimento.

A Figura 3-3 apresenta como o PMBOK visualiza os riscos de projeto.

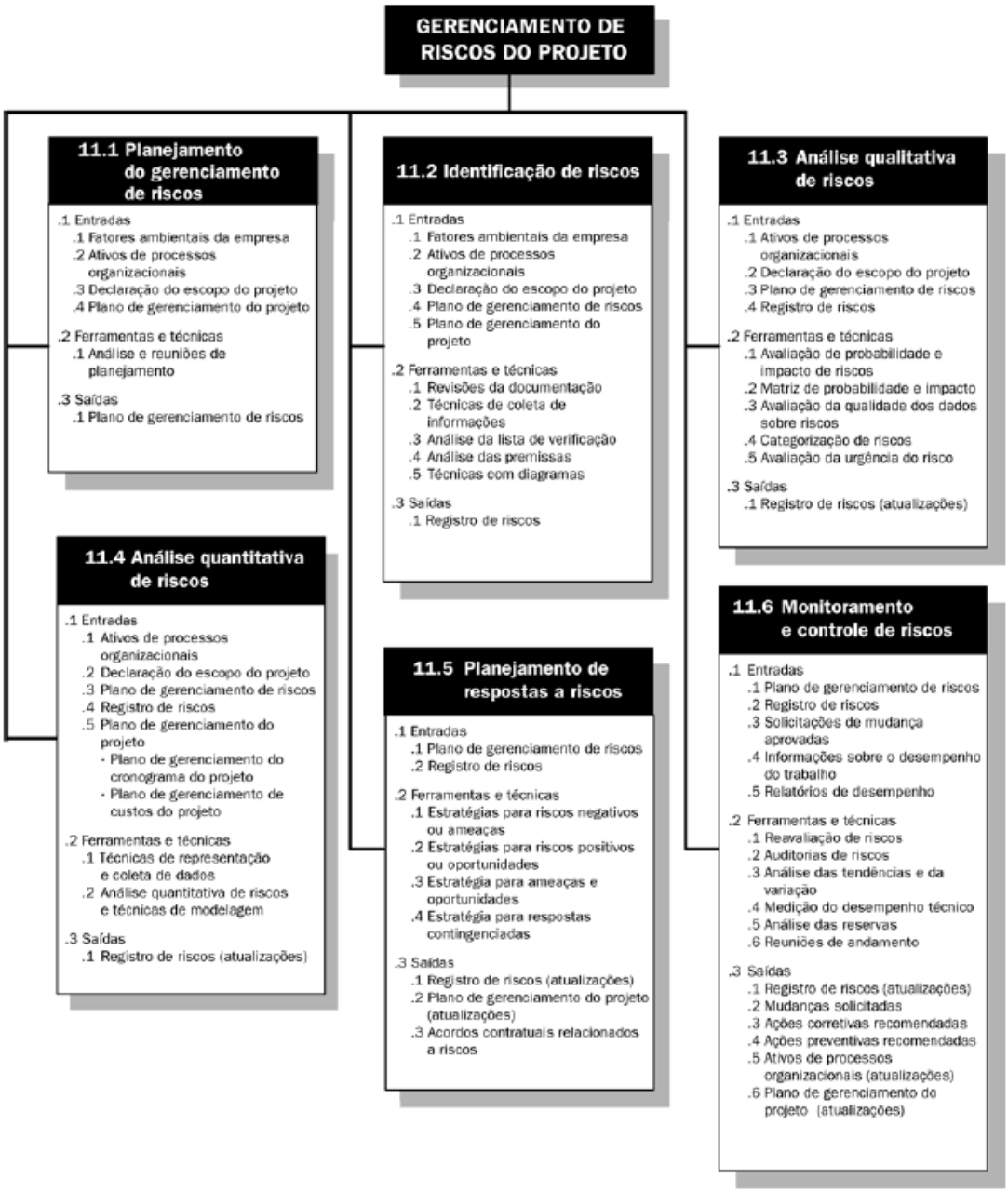


Figura 3-3 Visão geral do gerenciamento de riscos do projeto. (Fonte: PMI, 2004).

Para se planejar adequadamente o gerenciamento de riscos, o PMBOK indica um roteiro que pode ser parcialmente acoplado ao artefato a ser proposto. A seguir, os conceitos do PMBOK encontrados:

### 3.3.1 Como identificar riscos

Encontrar o nível, tipo e visibilidade do risco. Deve ser finalizado no início do planejamento do projeto e é uma das primeiras atividades a serem feitas.

- **Entradas**: Fatores ambientais da empresa, Ativos e processos organizacionais, Declaração de Escopo de Projeto, e Plano de gerenciamento do projeto, plano de gerenciamento de riscos do projeto.
- **Técnica**: Análise e reuniões de Planejamento, revisões de documentação, coleta de informações, Análise das premissas, uso de diagramas.
- **Saída**: Registro de riscos.

Para seguir esse plano de gerenciamento de riscos, é proposto um subconjunto de atividades, a saber:

- Metodologia;
- Responsabilidades;
- Orçamento;
- Cronograma;
- Definição de Probabilidade e Impacto;
- Categorização do Risco.

Essa categorização, segundo o PMI (2004) apresenta as categorias de riscos das quais fornecem estruturas que garantem um processo abrangente para se identificar riscos sistemicamente, até um nível consistente de detalhes. Isso contribui para a eficácia e qualidade da identificação dos riscos, que é o objetivo deste trabalho. Essa abordagem pode ser realizada simplesmente pela listagem de diversos aspectos do projeto (no caso deste trabalho, contratações de TI). As categorias de riscos podem ser reexaminadas durante todo o processo de identificação de riscos.

As informações que se basearem em projetos anteriores, necessitam de ajustes, adequações e ampliações para as novas situações aos quais estarão submetidas no novo projeto.

A Figura 3-4 apresenta a proposta do PMBOK para estruturar analiticamente os riscos.

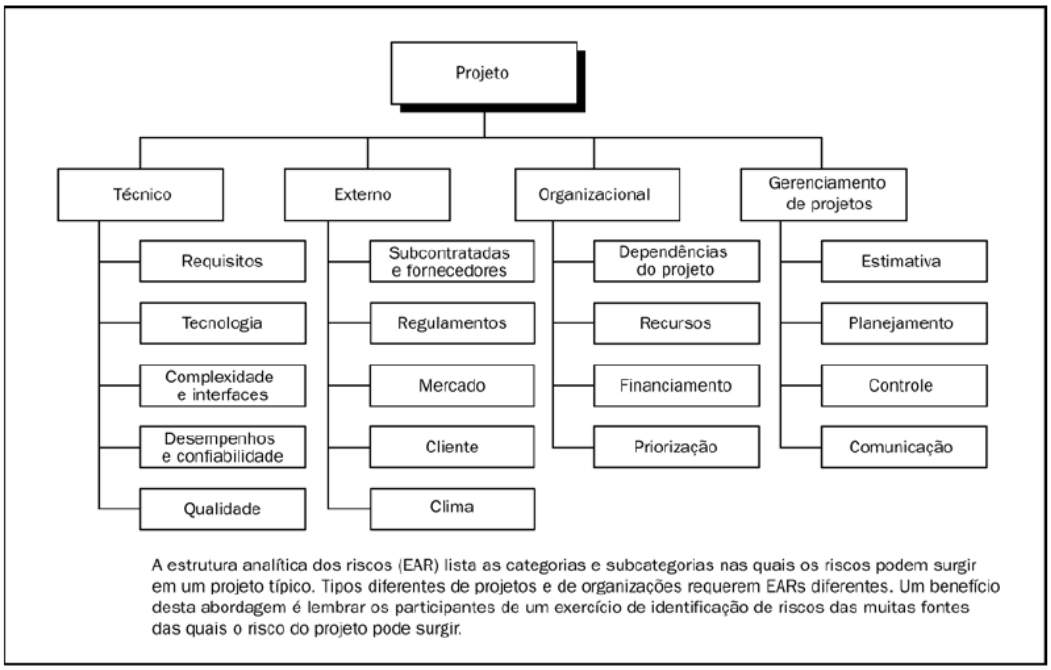


Figura 3-4 Estrutura analítica de riscos. (Fonte: PMI, 2004).

Poderá ser atribuída uma escala numérica ou uma matriz de probabilidade x impacto para definição de valores, mas como isso envolve a definição de escalas numéricas lineares e/ou não lineares, o trabalho se limitou a apoiar os gestores de TI na identificação dos riscos, pois o tratamento e classificação, muitas vezes seguem critérios culturais, quanto ao apetite para o risco, situação financeira e estratégias da organização, dentre outros. Seria necessária uma revisão bibliográfica muito mais extensa, caso fosse considerado o processo de gerenciamento de riscos do início ao fim, como preconiza a norma NBR 31000.

No contexto do gerenciamento de riscos, é fundamental que todos os envolvidos no projeto sejam incentivados a identificar riscos.

Este é um processo iterativo, pois novos riscos podem ser identificados durante o projeto.

Para identificação de riscos para o processo de contratação de TI, podem ser utilizadas várias técnicas dentre elas:

#### 3.3.1.1 Revisão de documentação

Verificar os planos de projeto pode permitir uma revisão estruturada, incluindo a revisão de projetos anteriores.

#### 3.3.1.2 Técnicas de coleta

- *Brainstorming*: Para se obter uma lista abrangente de riscos do projeto.
- Técnica *Delphi*: É um meio de alcançar um consenso entre os especialistas, onde anonimamente, por meio de um questionário e após várias rodadas, obtém-se o consenso, evitando-se influências no resultado.
- Matriz FOFA (Forças, Oportunidades, Fraquezas, Ameaças): Essa técnica pode aumentar a amplitude dos riscos considerados. Também chamada de matriz *SWOT*.
- Entrevistas: constitui-se numa das principais maneiras de se identificar riscos, por meio de pessoas mais experientes do projeto ou da organização.
- Identificação de Causa raiz: Investigação das causas essenciais dos riscos do projeto, que permite o agrupamento das causas, permitindo respostas adequadas à causa raiz de diversos riscos.
- Análise de listas de verificação: Verificação de análises históricas e do conhecimento que foi acumulado a partir de projetos anteriores. É uma lista que deve ser revisada ao fim do projeto.
- Análise das premissas: Os riscos são identificados pela análise de premissas que inicialmente são consideradas verdadeiras, mas com o decorrer do projeto, verifica-se o caráter inexato ou incompleto das premissas, identificando assim possíveis riscos.

#### 3.3.1.3 Técnicas com diagramas

- Diagramas de causa e efeito: Diagramas do tipo “espinha de peixe” (Ishikawa), servem para identificar as causas dos riscos.
- Fluxogramas: Mostram como se relacionam os mecanismos das causas.
- Diagramas de influência: representações gráficas de situações que mostram as influências causais, ordenando os eventos por tempo e outras relações de variáveis.

Essas análises para identificação de riscos permitem uma série de artefatos, dentre eles uma lista de riscos identificados, uma lista de possíveis respostas, lista de causa raiz, e as categorias do risco. Essas categorias podem ser sempre atualizadas, quando o artefato for solicitado.

## 3.4 ABNT NBR ISO 31000 - NORMA DE GESTÃO DE RISCOS

A GR não é uma atividade separada das principais atividades e processos da organização. Ela faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças (ABNT, 2009).

Todas as atividades de uma organização envolvem risco (ABNT, 2009). A GR é realizada com a identificação, análise, avaliação de tratamento do risco. Nesse processo, as partes interessadas são sempre informadas para assegurar que nenhum processo adicional de risco seja requerido.

A norma estabelece um número de princípios que precisam ser atendidos para tornar a GR eficaz (ABNT, 2009) e recomenda que para melhoria dos valores, políticas e da cultura organizacional das organizações, estas devem implantar e manter continuamente uma estrutura, com o intuito de integrar todos os processos para gerenciar riscos na governança, estratégia, planejamento e gestão. Essa visão vem ao encontro da visão do COBIT 4.1, exposta anteriormente.

Além disso, a norma realiza uma abordagem genérica, que pode ser aplicada em qualquer organização de qualquer setor em qualquer nível a qualquer momento. Essa realidade permitiu considerar essa norma para aplicação de seus conceitos teóricos na proposta de evolução do modelo de riscos da contratação brasileiro.

Uma das possibilidades com a implantação de GR é a possibilidade de uma gestão mais proativa, além de melhoria da governança, minimizar perdas, melhorar a aprendizagem organizacional e também o aumento da resiliência.

A norma considera ainda que as necessidades variadas de uma organização específica, seus objetivos, contexto, operações, processos, projetos, produtos, serviços ou ativos e práticas específicas empregadas, devem ser analisadas para a correta aplicação das estruturas de GR.

### 3.4.1 O modelo de riscos ABNT NBR ISO 31000

A GR tem sido desenvolvida ao longo do tempo e em muitos setores a fim de atender a várias necessidades. A norma permite que organizações públicas utilizem suas práticas em qualquer tipo de risco, independente de sua natureza (ABNT, 2009).

No Brasil, a ABNT é o Foro Nacional de Normalização, e a Comissão de Estudo Especial de GR foi a responsável pela elaboração da Norma ABNT NBR ISO 31000 (ABNT, 2009).

A aplicação da GR traz consigo necessidades particulares, vários tipos de público, percepções e critérios, de vários setores. Para contextualizar sua aplicação, a norma define que as organizações devem seguir etapas mínimas para gerenciar risco, tais como identificação, análise e avaliação do risco, para garantir a eficácia da GR.

A aderência à norma é analisada na ótica de desenvolver, implementar e melhorar continuamente uma estrutura que integre a GR na governança, estratégia, planejamento, processos de reportar dados e resultados, políticas, valores e cultura em toda a organização.

Entretanto, por ser uma norma genérica, ela não dita regras, mas sensibiliza sua aplicação com as devidas "customizações" para cada setor, por suas particularidades.

A definição de um contexto é a atividade chave da GR e essa atividade busca os objetivos da organização, o ambiente, partes interessadas, e demais critérios de risco, dos quais revelarão e avaliarão a natureza e a complexidade dos riscos.

A aplicação dos conceitos da norma pode aumentar as chances de atingir os objetivos e encorajar uma gestão proativa, melhorando a identificação de oportunidades e ameaças. Além disso, aplicando a norma, a organização poderá seguir o caminho para atendimento às diretrizes internacionais, requisitos legais e regulatórios pertinentes e melhorar o reporte das informações financeiras. Além disso, melhorar a confiança e a segurança 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, dentre outros, bem como a prevenção de perdas e a gestão de incidentes, e a melhoria da aprendizagem organizacional (ABNT NBR ISO 31000).

Com isso, verifica-se que caso se apliquem os conceitos de GR no modelo de análise de riscos da contratação de TI da APF, os resultados podem ser muito positivos.

Na Figura 3-5 é apresentado o modelo de relacionamento entre os princípios da GR, definidos pela ABNT NBR ISO 31000.

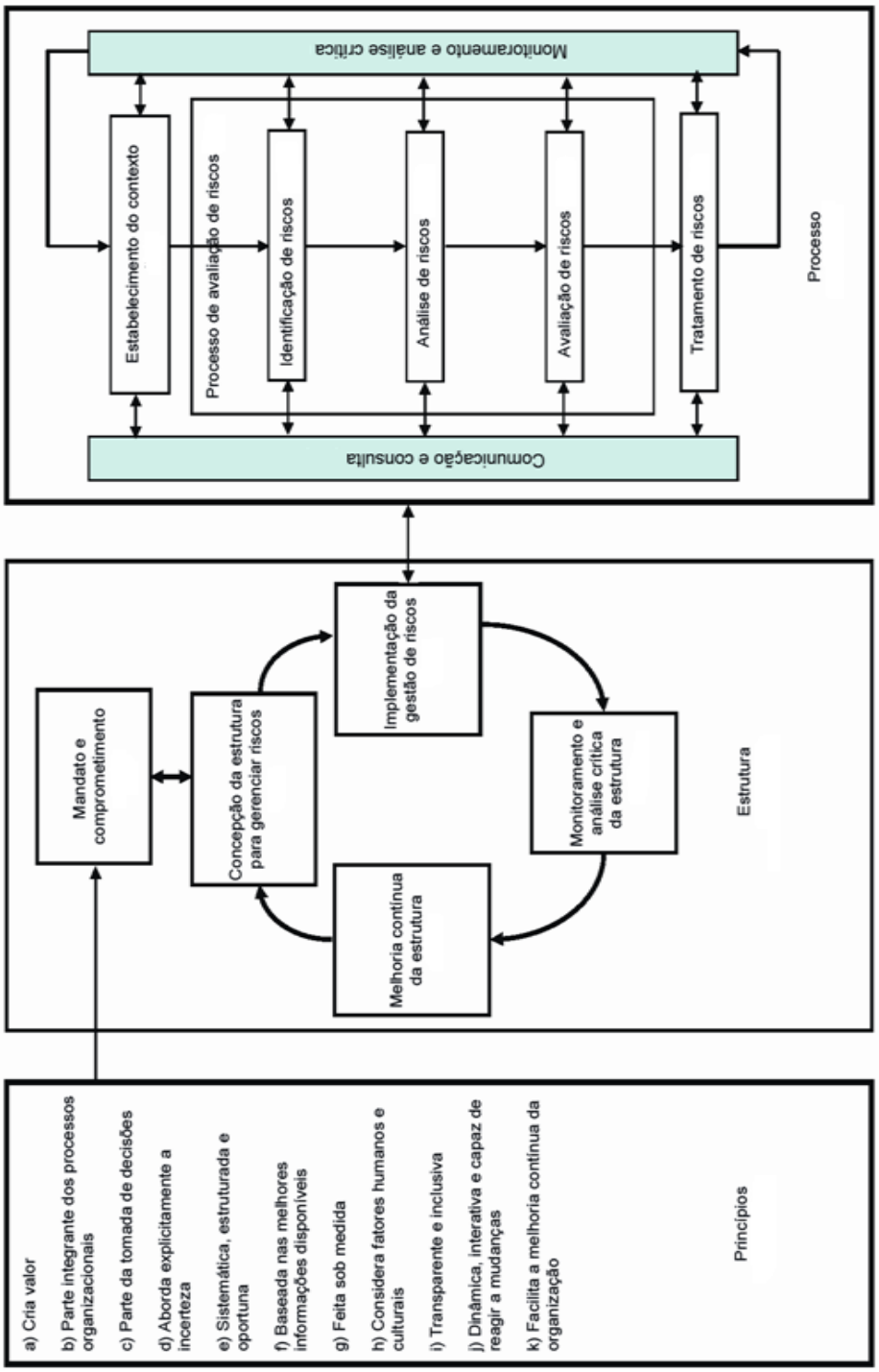

Figura 3-5 Relacionamentos entre os princípios da GR, estrutura e processo. (Adaptado de ABNT, 2009a)

Como já existe um modelo formal de análise de riscos específico para contratação de TI no Brasil, a norma sugere que nesse tipo de situação é conveniente a reavaliação e análise do documento em relação à ABNT NBR ISO 31000 para determinar sua suficiência e eficácia. E esta é uma das atividades deste trabalho, realizar a reavaliação do processo de identificação de riscos da contratação da APF no Brasil sob a ótica da ABNT NBR ISO 31000. Esse alinhamento será feito com o artefato, de acordo com o redesenho do processo de identificação de riscos apresentado no capítulo 2.

### 3.4.2 Por que considerar a ABNT NBR ISO 31000 com o artefato a ser proposto

Para propor um artefato baseado em premissas da norma ABNT NBR ISO 31000 é fundamental contextualizar os motivos que levaram a escolha desta norma para propor o artefato com este conteúdo em sua estrutura.

Primeiro, é importante destacar que a gestão de riscos é um tema vasto e a consolidação das ideias da gestão de riscos tem sido escrita ao longo dos anos por consenso de vários segmentos e profissionais, compilados no documento da ABNT NBR ISO 31000. Esta norma foi aprovada por instituição reconhecida internacionalmente, visando um grau ótimo da qualidade das informações.

A norma é reguladora e orientativa, para que os gestores de risco tenham uma diretriz a ser seguida.

Ela começou há aproximadamente 45 anos, com o advento das normas de qualidade do exército americano. Tal norma foi revisada em 1971 e 1978. O Canadá, no ano de 1985, realizou  outra revisão do documento.

Foi gerada assim a norma ABS5750, que tratava sobre requerimentos de qualidade.

A partir daí, uma série de normas, revisões e países entraram no cenário, e, em resumo destaca as seguintes normas:

- SA 8000 – Sustentabilidade (1997).
- OHSAS 18001 - Segurança do trabalho (1999).
- Norma 4360 - Primeira norma de Gestão de Riscos no mundo (Austrália) (1999).
- ISO 9001 - ISO da qualidade (2000).
- Norma 4360 - Revisão - Enquadrou a norma como *framework* (2004).
- ISO 14001 - Meio Ambiente (2004).

- ISO 9001 - ISO da qualidade - Segunda revisão (2005).
- BS 25999 - Continuidade de negócio (2007).
- ISO 9001 - ISO da qualidade - Terceira revisão (2008).

Com esse histórico e com base na percepção da existência de riscos globais (não só nas empresas, mas também de uma maneira holística) foi então criada a Norma ABNT NBR ISO 31000.

Esta norma se fundamenta em pilares de preocupação global (riscos globais), na seguinte ordem:

1. Sistema financeiro.
2. Segurança do meio ambiente integrado com alimentar.
3. Cadeia de fornecimento (energia, indústrias, infraestrutura).
4. Terrorismo.

Esses quatro riscos fizeram que a ISO 31000 fosse criada de maneira ainda mais rápida. Isso vem ao encontro também ao problema de vários padrões falarem linguagens de riscos diferentes, o que causa um conflito terminológico, consenso e de padrões, que necessitava de maior atenção.

A norma foi criada com o princípio de atender toda empresa de qualquer porte e serve para organizações de todos os segmentos. Tem a característica explorar as incertezas, que podem afetar os objetivos empresariais e de negócio das organizações, de maneira abrangente, envolvendo desde a parte financeira, operação, saúde do trabalhador, segurança da informação, dentre outros aspectos que possuíam matrizes de riscos diferentes, gerando várias "ilhas" de gestão de riscos.

A ABNT NBR ISO 31000, possui uma visão moderna, que trata tanto o lado negativo do risco (perda) quanto o lado positivo (oportunidade). Possui o desafio de estabelecer linguagem comum, padronizar as melhores práticas e uma abordagem convergente para implementação prática, por meio de um *framework*, que possui sete passos:

1. Comunicação e consulta;
2. Estabelecimento do contexto;
3. Perigos de fatores de riscos;
4. Análise de riscos (critério de probabilidade x impacto);

5. Classificação (Avaliação de risco);
6. Tratamento do risco (via uma matriz com quantos quadrantes necessários);
7. Responder aos riscos;
8. Monitoramento da resposta.

Este ciclo segue a filosofia do PDCA (*Plan-Do-Check-Act*), sendo retroalimentado durante todo seu ciclo de vida.

O motivo de escolha desta norma, além dos motivos acima apresentados, foi consenso entre 35 países, incluindo Brasil, por meio da ABNT, para criação da norma.

Um trabalho que seguiu uma política multidisciplinar, com atores de áreas como Governança Corporativa, Área Financeira, Seguros, Segurança Empresarial, Segurança do Trabalho, Qualidade, Meio Ambiente, TI e Agronegócios, dentre muitas outras, foi outro fator o que motivou a busca do alinhamento do modelo de Análise de Riscos atual com o estado da arte na gestão de riscos, por meio da construção de um artefato para Identificação de Riscos, que poderá contribuir com uma parcela considerável do processo de contratação de TI da APF.

Além disso, deve-se observar que a norma de gestão de riscos, deve criar valor, ser parte integrante de qualquer processo (inclusive da identificação de riscos), tem que ser um processo decisório, tem que tratar a incerteza claramente, tem que ser sistemática e estruturada (retroalimenta), basear-se na melhor informação possível, ser customizável (sem gerar custos), considerar o fator humano (não focar na tecnologia - utilizar lógica intuitiva), ser transparente e incluir as partes interessadas, além de dinâmica e interativa, na busca de responder a mudança, seguindo uma política de melhoria contínua, sendo assim, aberta a melhorias.

Essas considerações permitiram escolher a norma ABNT NBR ISO 31000 para prover insumos para a criação de um artefato de Identificação de Riscos para as contratações de TI, pois ela poderá inserir informações importantes no processo de Análise de Riscos da IN04.

## 3.5 ABNT NBR ISO GUIA 73 – GESTÃO DE RISCOS – VOCABULÁRIO

A norma ABNT NBR ISO GUIA 73 fornece o vocabulário básico para desenvolver um entendimento comum sobre os termos e conceitos de GR entre organizações e funções.

Ela inclui a definição de termos genéricos relativos à GR e destina-se a incentivar uma compreensão mútua e consistente além uma abordagem coerente na descrição das atividades relativas à GR e a utilização de terminologia uniforme de GR em processos e estruturas para gerenciar riscos. O guia tem como objetivo envolver pessoas que gerenciam riscos e que estão envolvidas em atividades da ISO e IEC, além de desenvolvedores de normas, guias, procedimentos e códigos de prática relativos à GR nacional ou de setores específicos.

Para a norma, a identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

A harmonização terminológica que será apresentada em 4.2 irá aplicar os conceitos da ABNT NBR ISO Guia 73 nos termos inseridos pelo guia de contratações de TI da APF.

### 3.6 ABNT NBR ISO 31010 – TÉCNICAS DE AVALIAÇÃO DE RISCOS

A norma ABNT NBR ISO 31010, trata do processo de avaliação de riscos, que é o processo global de identificação de riscos, análise de riscos e avaliação de riscos. Riscos podem ser avaliados em nível organizacional, em nível departamental, para projetos, atividades individuais ou riscos específicos. Diferentes ferramentas e técnicas podem ser apropriadas em diferentes contextos (ABNT, 2012).

O processo de avaliação de riscos possibilita um entendimento dos riscos, suas causas, consequências e probabilidades. Isto proporciona uma entrada para decisões sobre:

- Se convém que uma atividade seja realizada;
- Como maximizar oportunidades;
- Se os riscos necessitam ser tratados;
- A escolha entre opções com diferentes riscos;
- A priorização das opções de tratamento de riscos;
- A seleção mais apropriada de estratégias de tratamento de riscos que trará riscos adversos a um nível tolerável.

Este trabalho não irá definir um método único para se identificar riscos das contratações, mas a norma ainda pode dar um apoio significativo, pois recomenda quais as técnicas podem ou não ser aplicadas em cada fase da GR. Não há restrições para utilizar as práticas da norma para contratações de TI, entretanto a Análise de Riscos da IN04 propõe a técnica

de matriz de ‘probabilidade x dano x impacto’, referenciada na norma ABNT NBR ISSO 31010.

A Tabela 3-2, extraída da norma ABNT NBR ISO 31010, apresenta quais as metodologias de identificação de riscos são recomendadas e que podem ser aplicadas também para identificação de riscos nas contratações de TI, pois a norma também se refere à aplicação em qualquer organização.

Foram destacadas somente as metodologias que possuem forte recomendação, segundo a própria ABNT NBR ISO 31010, de serem aplicadas em todas as fases do processo de GR.

**Tabela 3-2** Aplicação de ferramentas e técnicas para avaliação de riscos. (Fonte: ABNT, 2012).

| Tools and techniques | Risk assessment process | | | | | See Annex |
|---|---|---|---|---|---|---|
| | Risk Identification | Risk analysis | | | Risk evaluation | |
| | | Consequence | Probability | Level of risk | | |
| Brainstorming | SA[1)] | NA[2)] | NA | NA | NA | B 01 |
| Structured or semi-structured interviews | SA | NA | NA | NA | NA | B 02 |
| Delphi | SA | NA | NA | NA | NA | B 03 |
| Check-lists | SA | NA | NA | NA | NA | B 04 |
| Primary hazard analysis | SA | NA | NA | NA | NA | B 05 |
| Hazard and operability studies (HAZOP) | SA | SA | A[3)] | A | A | B 06 |
| Hazard Analysis and Critical Control Points (HACCP) | SA | SA | NA | NA | SA | B 07 |
| Environmental risk assessment | SA | SA | SA | SA | SA | B 08 |
| Structure « What if? » (SWIFT) | SA | SA | SA | SA | SA | B 09 |
| Scenario analysis | SA | SA | A | A | A | B 10 |
| Business impact analysis | A | SA | A | A | A | B 11 |
| Root cause analysis | NA | SA | SA | SA | SA | B 12 |
| Failure mode effect analysis | SA | SA | SA | SA | SA | B 13 |
| Fault tree analysis | A | NA | SA | A | A | B 14 |
| Event tree analysis | A | SA | A | A | NA | B 15 |
| Cause and consequence analysis | A | SA | SA | A | A | B 16 |
| Cause-and-effect analysis | SA | SA | NA | NA | NA | B 17 |
| Layer protection analysis (LOPA) | A | SA | A | A | NA | B 18 |
| Decision tree | NA | SA | SA | A | A | B 19 |
| Human reliability analysis | SA | SA | SA | SA | A | B 20 |
| Bow tie analysis | NA | A | SA | SA | A | B 21 |
| Reliability centred maintenance | SA | SA | SA | SA | SA | B 22 |
| Sneak circuit analysis | A | NA | NA | NA | NA | B 23 |
| Markov analysis | A | SA | NA | NA | NA | B 24 |
| Monte Carlo simulation | NA | NA | NA | NA | SA | B 25 |
| Bayesian statistics and Bayes Nets | NA | SA | NA | NA | SA | B 26 |
| FN curves | A | SA | SA | A | SA | B 27 |
| Risk indices | A | SA | SA | A | SA | B 28 |
| Consequence/probability matrix | SA | SA | SA | SA | A | B 29 |
| Cost/benefit analysis | A | SA | A | A | A | B 30 |
| Multi-criteria decision analysis (MCDA) | A | SA | A | SA | A | B 31 |

[1)] Strongly applicable.
[2)] Not applicable.
[3)] Applicable.

A junção de técnicas ou a combinação delas poderá prover uma identificação de riscos cada vez mais aprimorada. Isso dependerá somente do interesse do gestor responsável pela contratação em aplicar as técnicas que estiverem sob seu alcance.

O modelo de Análise de Riscos da contratação da APF já utiliza a matriz de probabilidade x dano x impacto (Figura 2-11), que é uma matriz similar a de Probabilidade e Consequência (acima destacada). Este trabalho não irá propor uma mudança na metodologia atualmente utilizada de classificação de riscos, por verificar que o modelo de análise de risco brasileiro utiliza parcialmente uma referência da ABNT NBR ISO 31010.

# 4. CONSTRUÇÃO DO ARTEFATO DE IDENTIFICAÇÃO DE RISCOS

Este capítulo apresenta como foi realizada a extração das premissas para a construção do artefato de Identificação de Riscos.

## 4.1 MODELO DE CONSTRUÇÃO DO ARTEFATO

Para o início da construção, será inicialmente apresentado o modelo atual de planejamento da contratação, devidamente estruturado com premissas (PMI, 2004) originadas de fontes referenciadas neste trabalho, em estrutura de árvore, com uso da ferramenta *Freemind*, para definição das categorias de informação que podem ser adotadas para se identificar os riscos. Tal ferramenta permite a construção de estruturas em árvores e mapas mentais, caracterizando assim a proposta de um artefato, pois irá aprimorar o modelo atual, inserindo no artefato as principais características que devem ser consideradas. Com o uso da ferramenta foram criados mapas mentais com as premissas referenciadas pela norma ABNT NBR ISO 31000, além de mapeado o processo atual de contratação de TI para normalização das informações.

As Figuras 4-1 a 4-6 a seguir apresentam o detalhamento das premissas mapeadas do processo de Contratação de TI para construção do artefato de Identificação de Riscos.

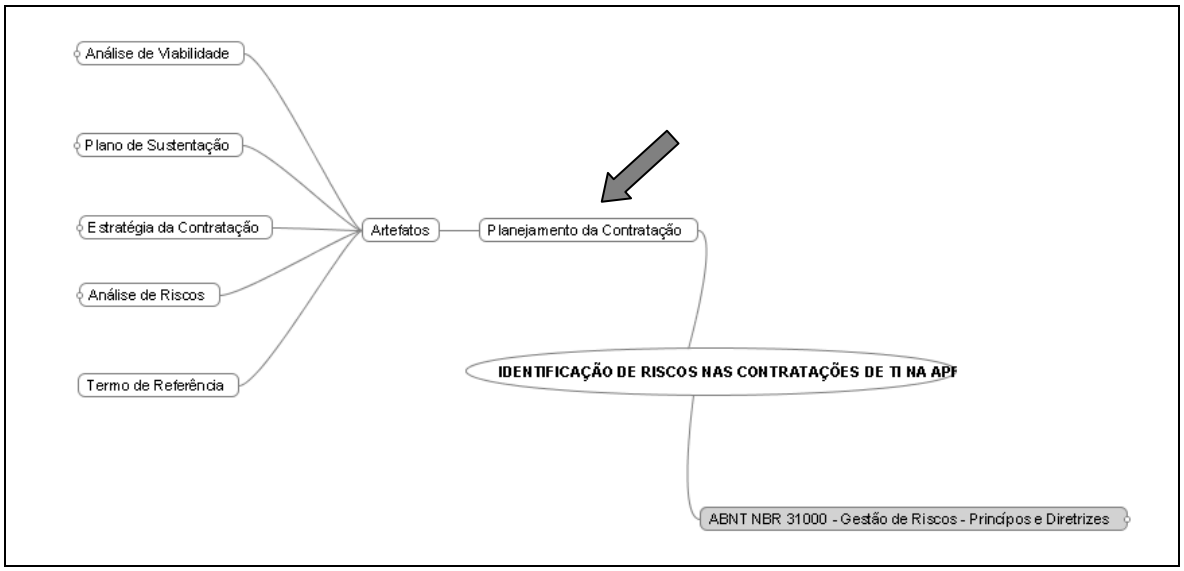


Figura 4-1 Visão do processo na fase de Planejamento da Contratação: Artefatos.

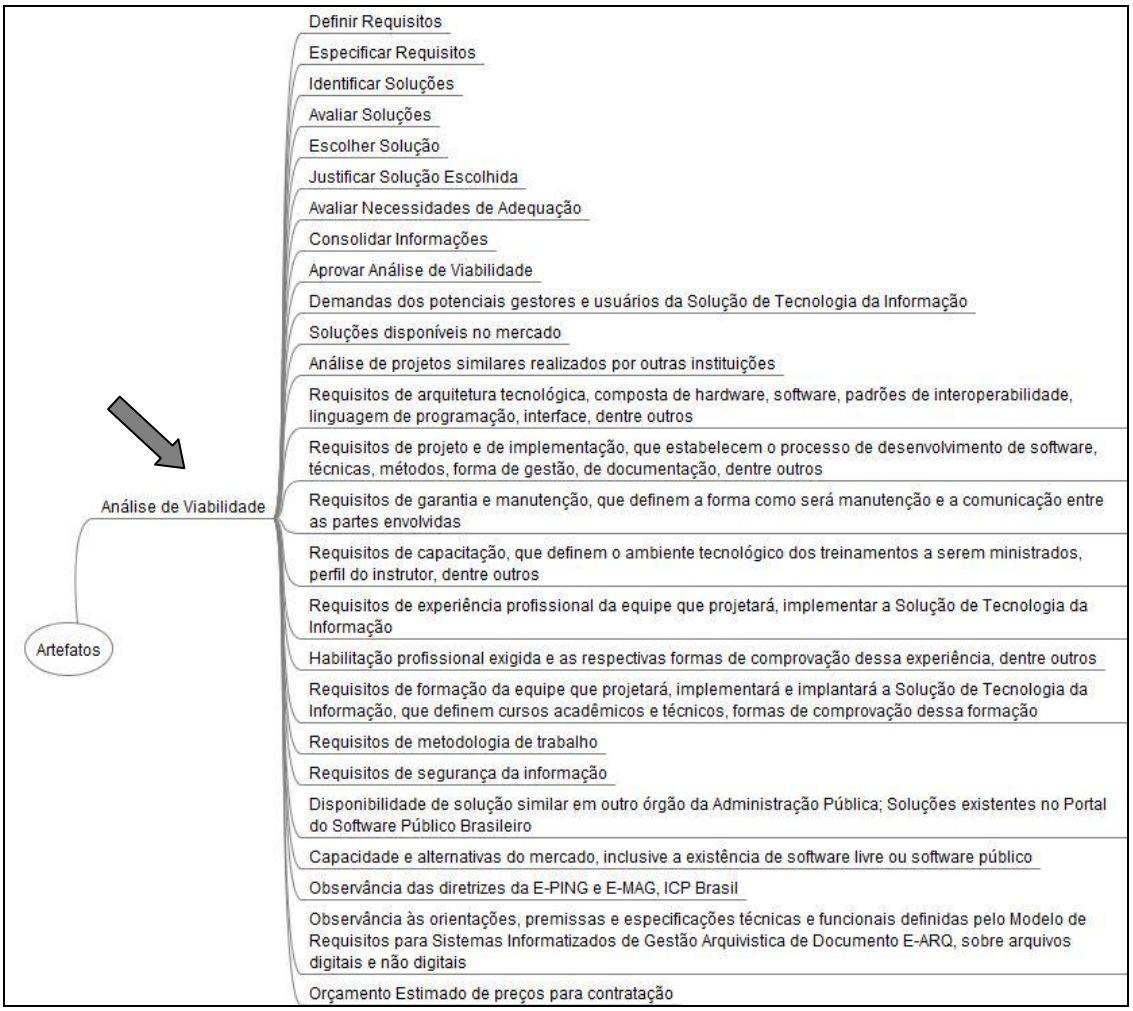


Figura 4-2 Mapa mental da Análise de Viabilidade.

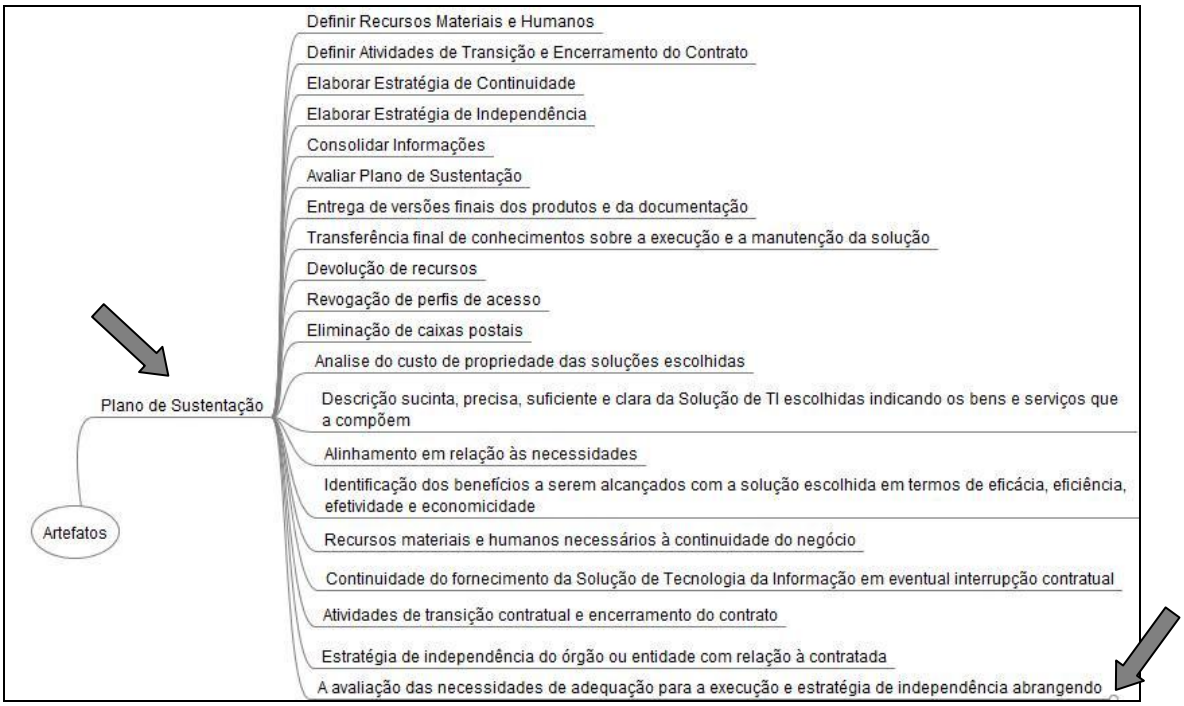


Figura 4-3 Mapa mental do Plano de Sustentação.

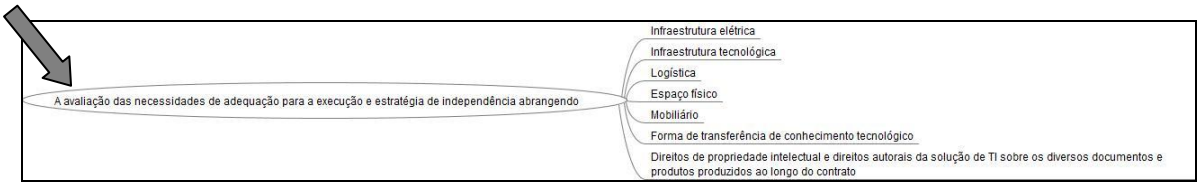


Figura 4-4 Mapa mental do Plano de Sustentação (detalhamento)

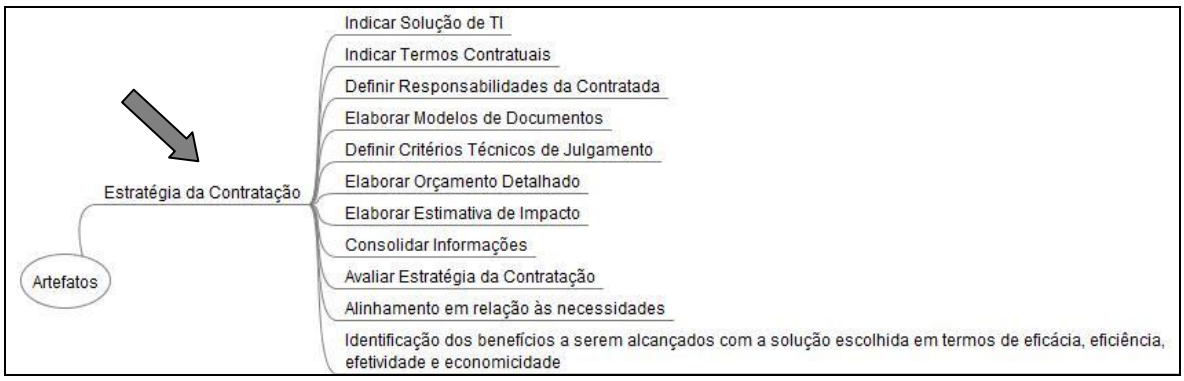


Figura 4-5 Mapa mental da Estratégia da Contratação.

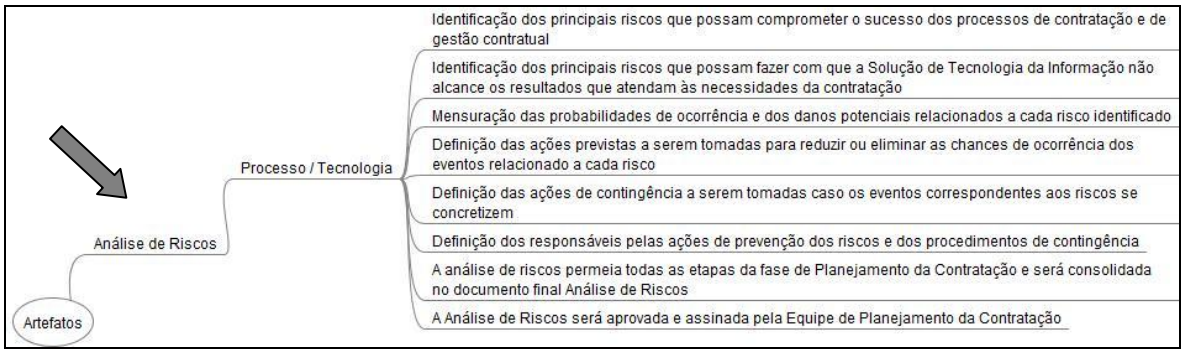


Figura 4-6 Mapa mental da Análise de Riscos.

Os processos acima descritos são originados do Guia Prático para Contratação de Soluções de TI e foram desenhados na estrutura de árvore para fins de comparação das atividades correlatas.

Para propor um artefato alinhado às práticas e normas de riscos foram levantados na revisão bibliográfica todos os conceitos e informações que pudessem agregar novas atividades da norma ABNT NBR ISO 31000, do PMBOK, COBIT dentre outros autores que foram frutos da pesquisa e puderam ter as ideias consideradas para a construção do artefato. Esse foi o parâmetro para escolha dos itens que compuseram as árvores que motivaram o artefato (autores que abordaram o tema). Essa prática servirá para que o gestor possa definir quais os conceitos podem ser considerados, utilizando-se de outras

opiniões e definições caso seja necessário, para a diminuição de riscos da especificação em questão. As figuras 4-7 a 4-23 apresentam as compilações apontadas pelas normas, modelos, autores e referências.

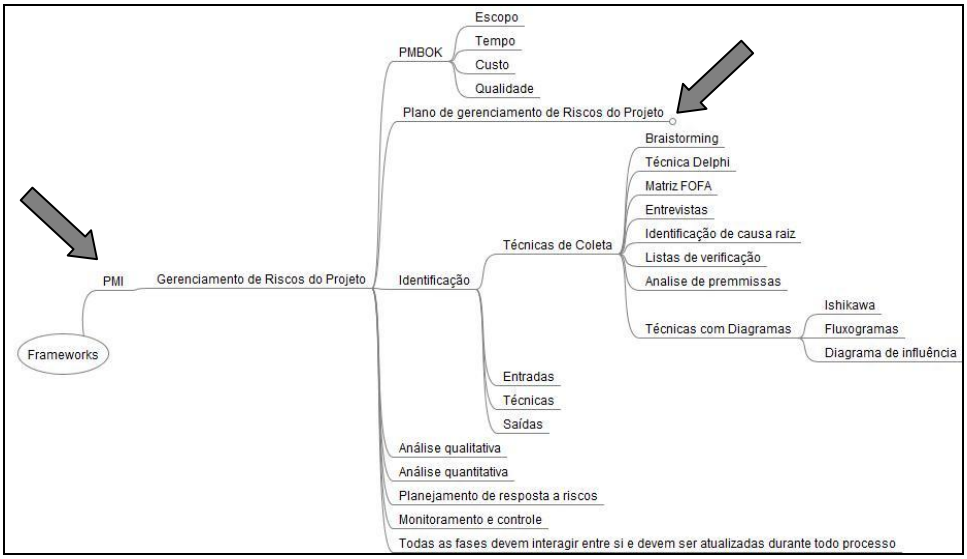


Figura 4-7 Mapa mental do PMBOK (2004)

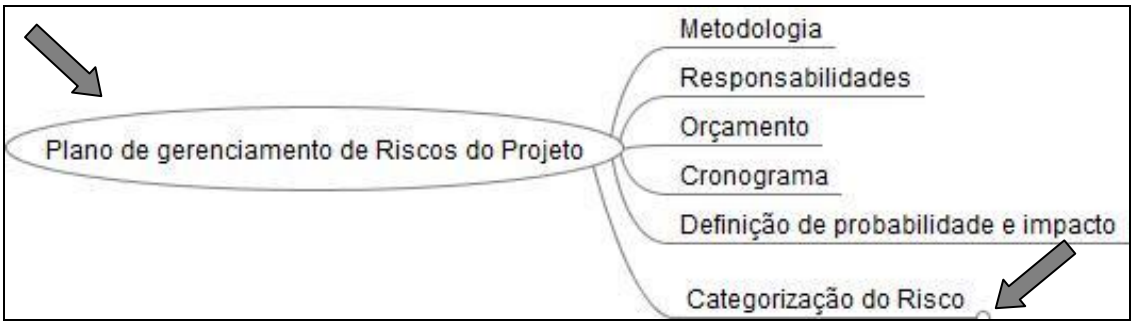


Figura 4-8 Mapa mental do PMBOK (2004) (detalhamento)

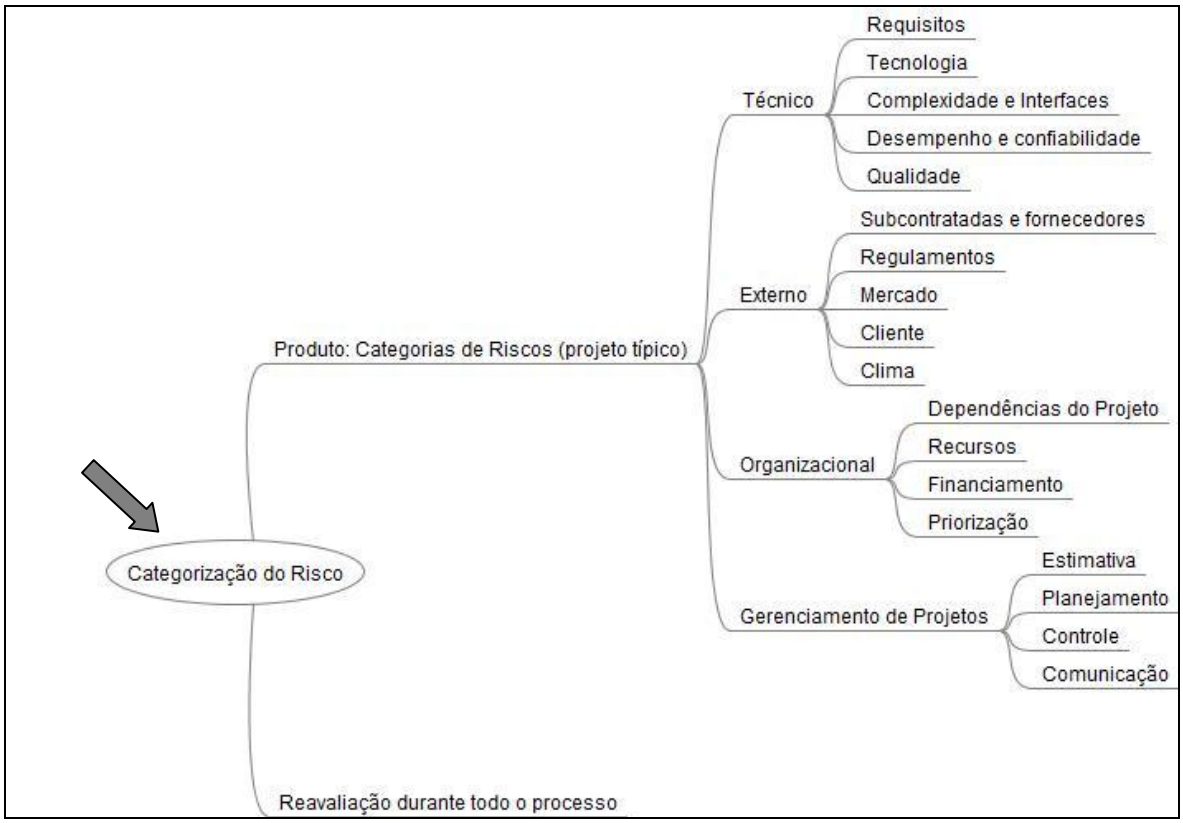


Figura 4-9 Mapa mental do PMBOK (2004) (sub-detalhamento)

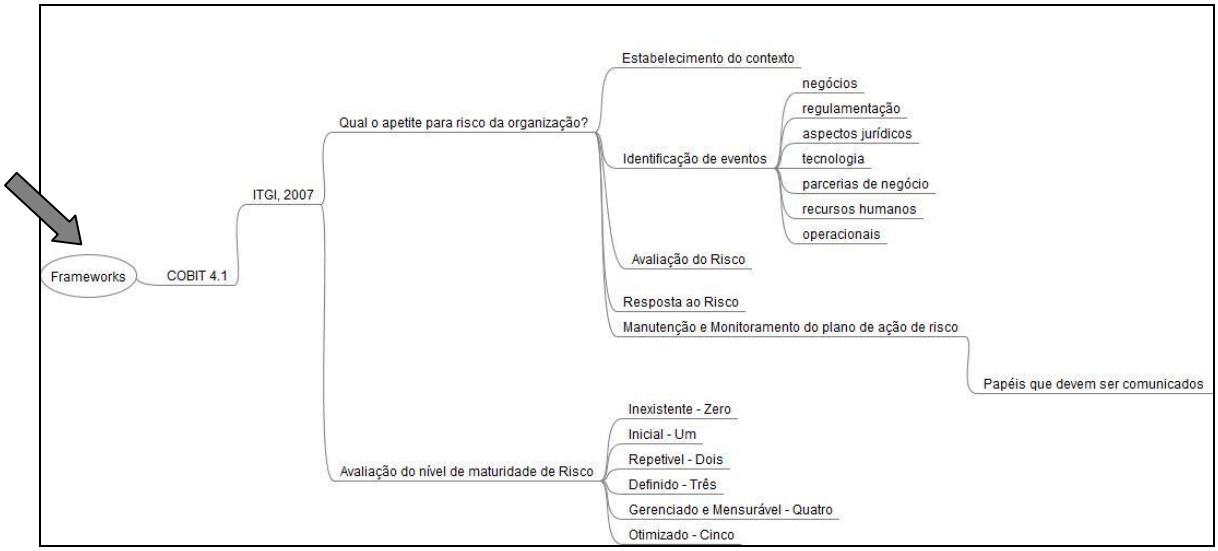


Figura 4-10 Mapa mental COBIT 4.1.


Figura 4-11 Mapa mental ABNT NBR ISO 31000 (1).

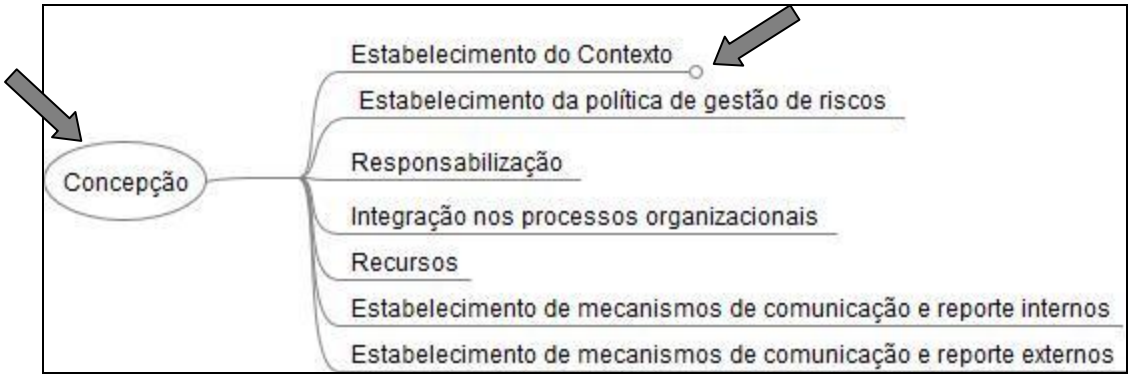


Figura 4-12 Mapa mental ABNT NBR ISO 31000 (2).

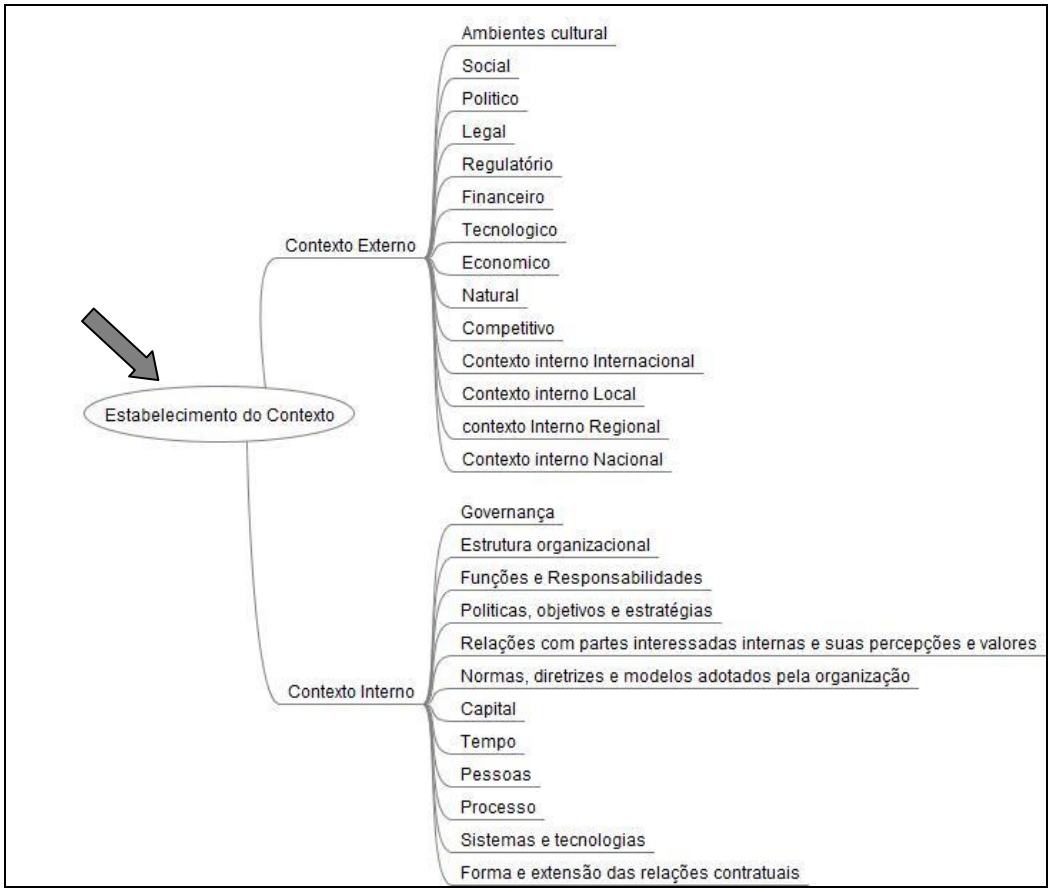


Figura 4-13 Mapa mental ABNT NBR ISO 31000 (3).

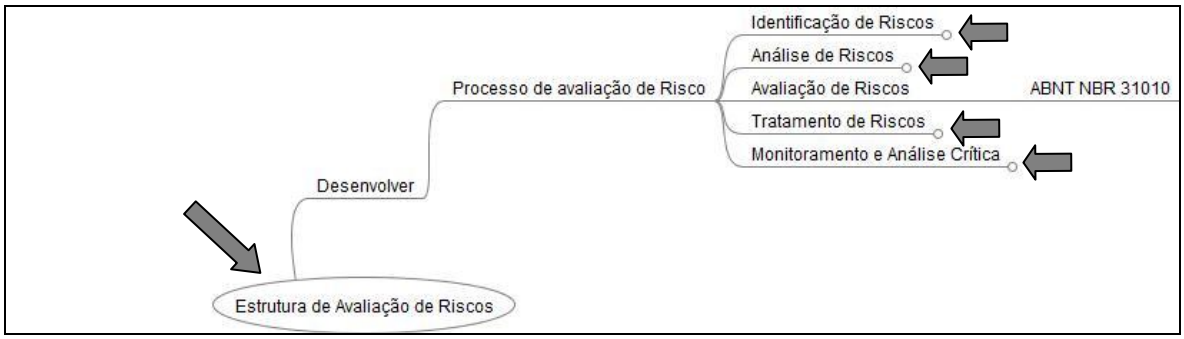


Figura 4-14 Mapa mental ABNT NBR ISO 31000 (4).

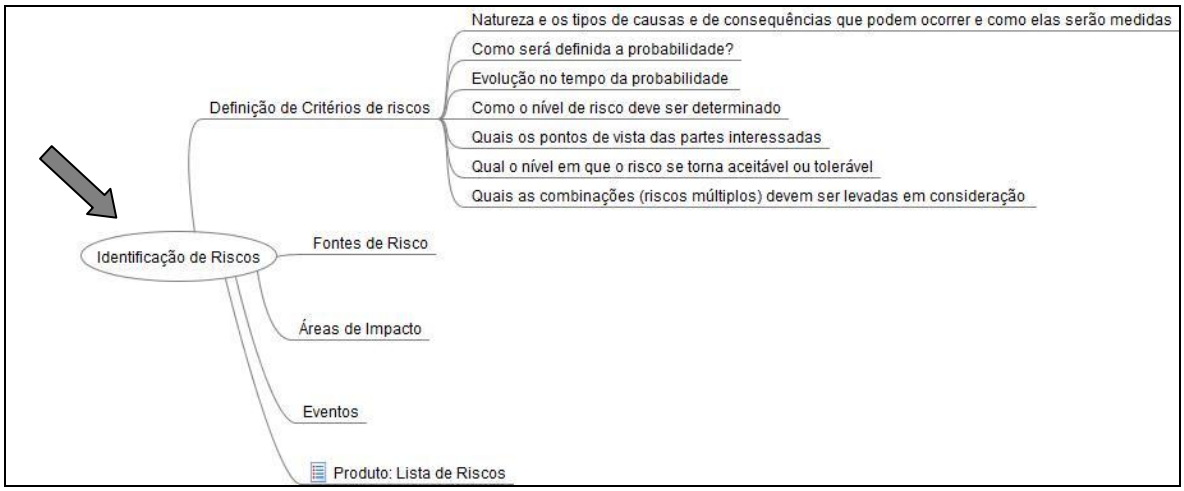


Figura 4-15 Mapa mental ABNT NBR ISO 31000 (5).


Figura 4-16 Mapa mental ABNT NBR ISO 31000 (6).

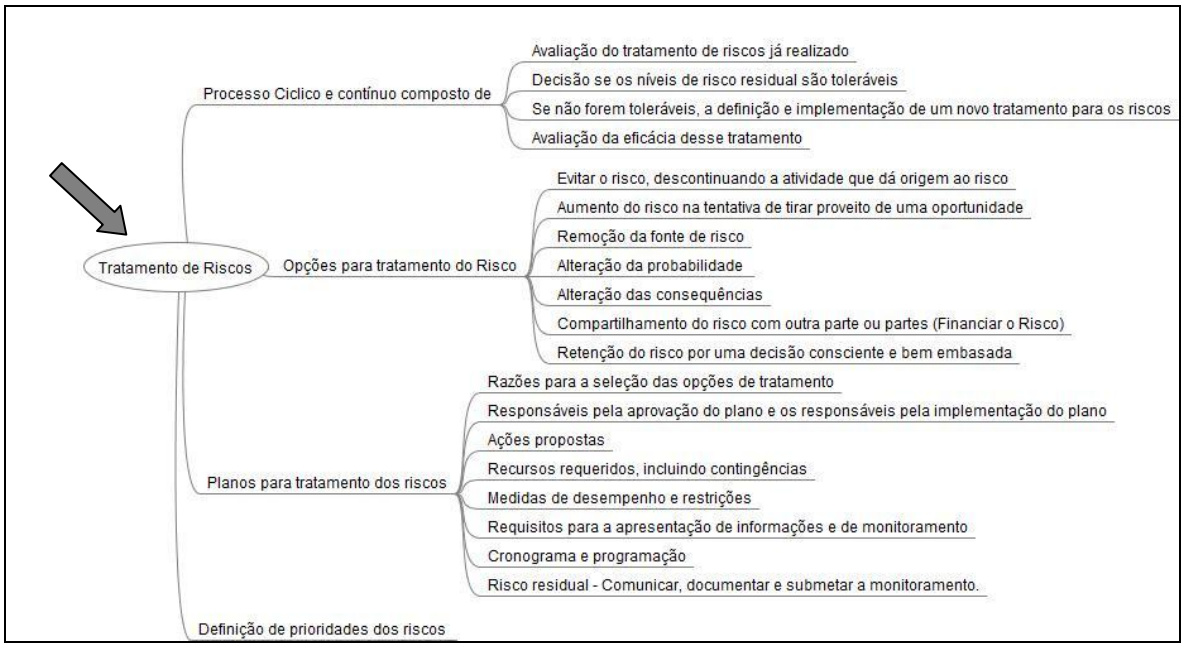


Figura 4-17 Mapa mental ABNT NBR ISO 31000 (7).

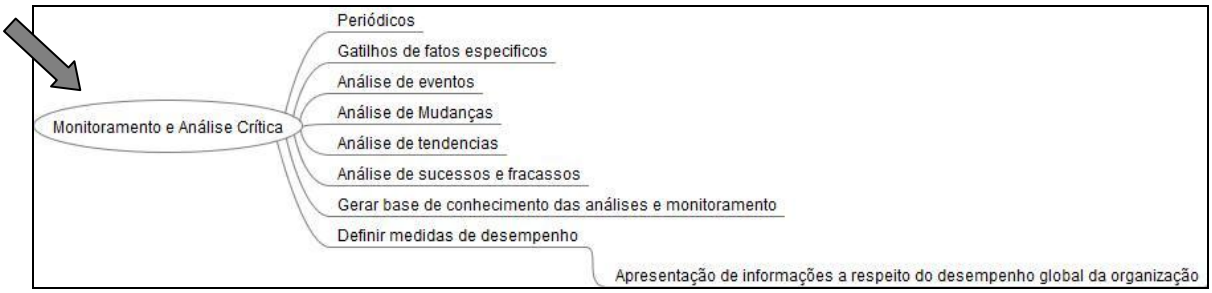


Figura 4-18 Mapa mental ABNT NBR ISO 31000 (8).


Figura 4-19 Mapa mental ABNT NBR ISO 31000 (9)

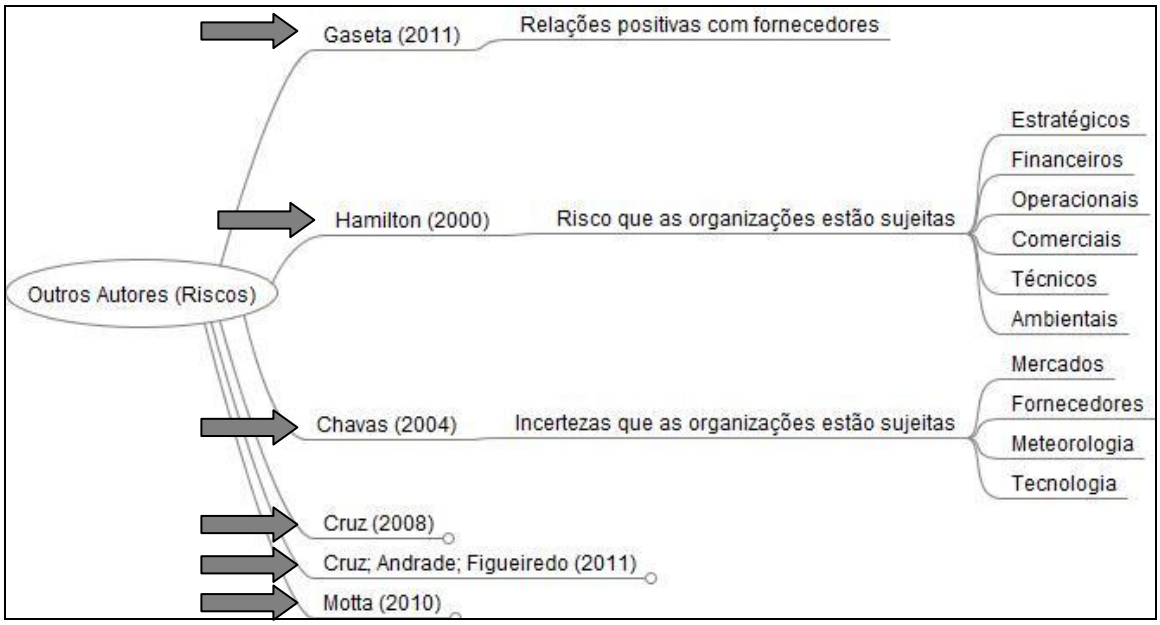


Figura 4-20 Mapa mental com a visão de outros autores sobre riscos

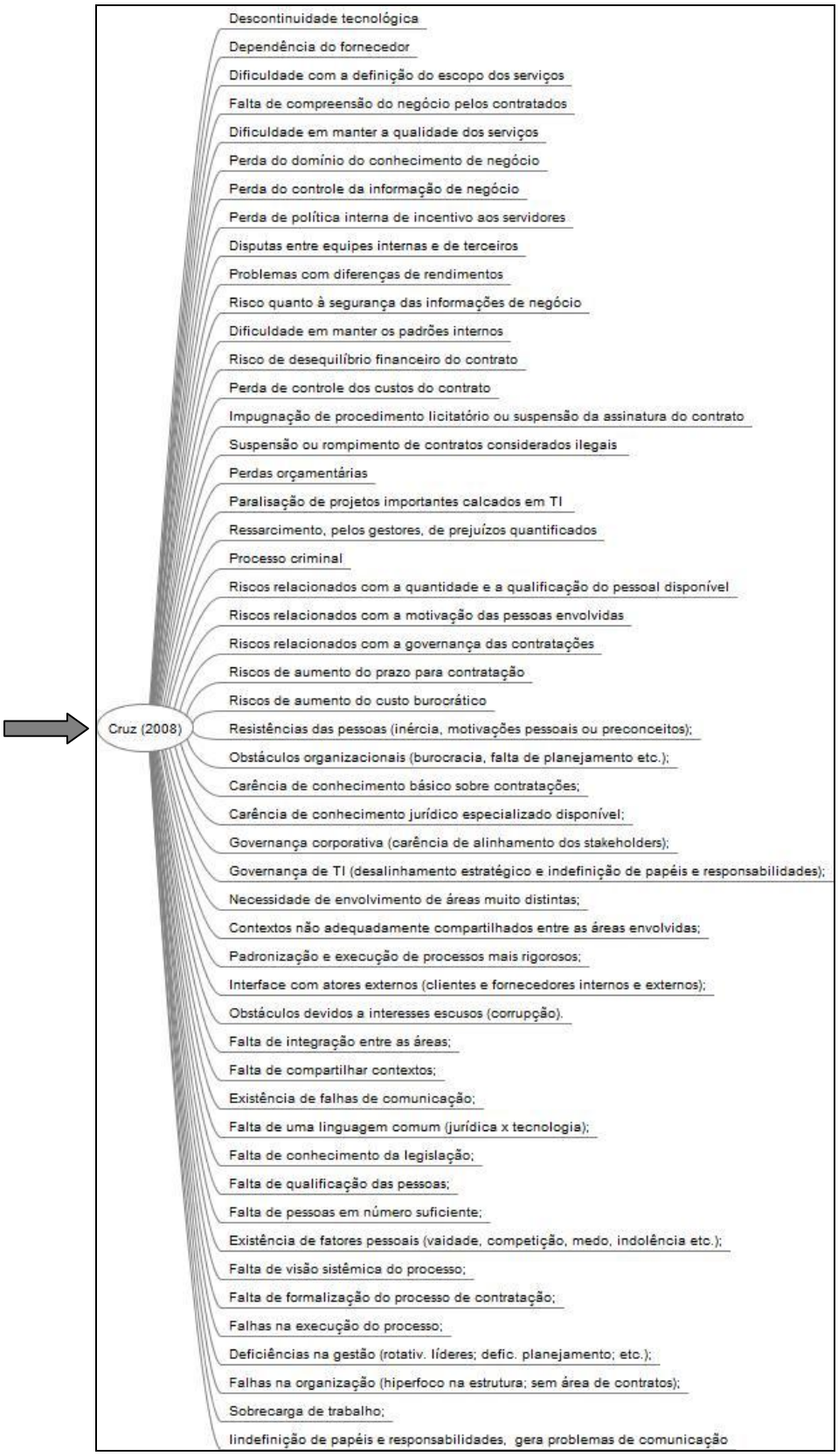


Figura 4-21 Mapa mental com a visão de Cruz (2008)


Figura 4-22 Mapa mental com a visão de visão de Cruz, Andrade e Figueiredo (2011)

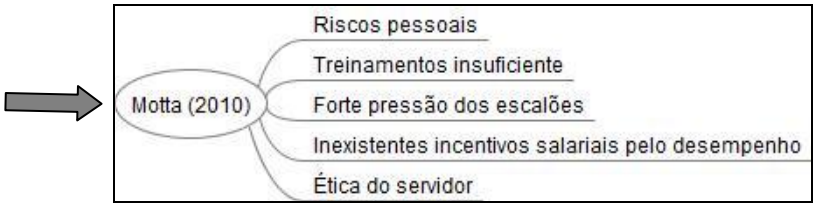


Figura 4-23 Mapa mental com a visão de visão de Motta (2010)

Cada premissa dos mapas mentais foi classificada como um "conceito" selecionado do estado da arte. Os conceitos estão em níveis de atividades de 1º e 2º nível, sendo o 1º nível sobre princípios e conceitos e o segundo nível sobre atividades.

Pode-se utilizar qualquer um dos níveis para composição de categorias de informação, o que permitirá ao gestor optar por considerar ou não o critério, adequando a semântica do texto para este fim.

Este mapa mental foi construído baseado na leitura e interpretação dos itens que descrevem as normas citadas neste trabalho. Caso seja necessário adaptar o método para uso de outras referências, é possível que se faça o mesmo levantamento para adequação das atividades com o objetivo necessário.

Com essas condições, será proposta uma harmonização terminológica dos termos atualmente utilizados. A seguir será criado o novo artefato para Identificação de Riscos nas contratações de TI para APF, baseado nos mapas mentais elaborados.

## 4.2 HARMONIZAÇÃO TERMINOLÓGICA

Os conceitos e os termos evoluem de modo diferente nas línguas e nas comunidades linguísticas, em função de diversos fatores históricos, geográficos, sociais ou econômicos,

dentre outros (ABNT, 1997). Essas variações apresentam pseudo-semelhanças entre os termos que prejudicam a comunicação internacional.

Essas diferenças entre os termos existem, pois cada conceito pode estar em um nível diferente. As similaridades nos termos não significa que sejam idênticos, pois existem termos e conceitos elaborados para o emprego e uso internacional mas que podem ser inadmissíveis no cenário nacional (ABNT, 1997). A ABNT (1997) considera que atividade de redução ou eliminação de pequenas diferenças entre dois ou mais conceitos muito similares se denomina "harmonização de conceitos".

A harmonização terminológica é a atividade que irá apresentar quais os conceitos que poderiam ser utilizados pelo modelo atual, para que este siga as diretrizes da GR. Para realizar o alinhamento dos campos contidos no *template* de Análise de Riscos será adotado o seguinte procedimento:

1. Listagem dos campos atuais.
2. Alinhamento (de-para) dos termos sugeridos pela ABNT NBR ISO GUIA 73, que trata do vocabulário para gestão de riscos, sob ótica da norma NBR 13790 - Terminologia - Princípios e Métodos - Harmonização de conceitos e termos.

A norma NBR 13790 segue o fluxo definido na Figura 4-20 para normalização de um conceito:

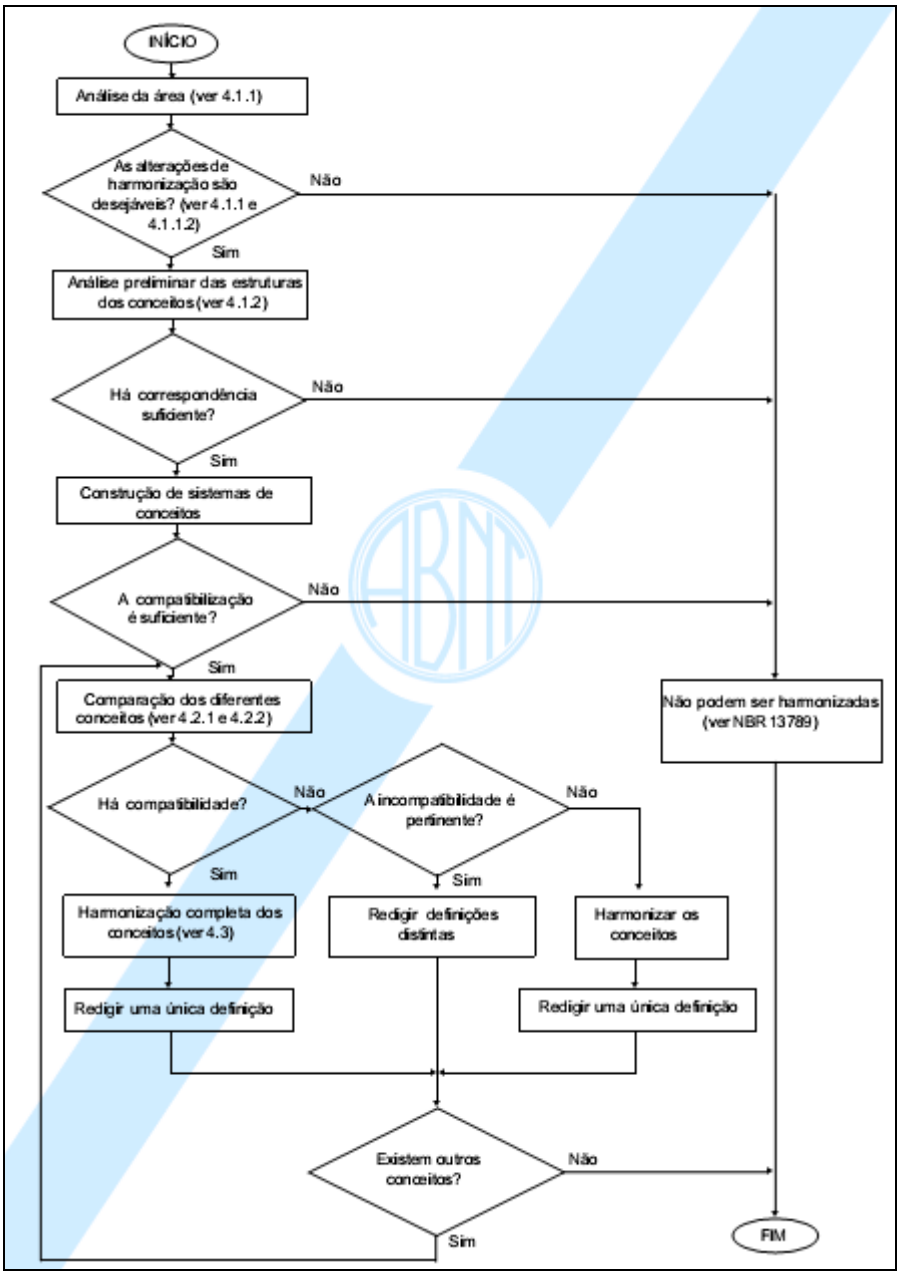


Figura 4-24 Procedimento de Harmonização Terminológica. (Fonte: ABNT, 1997).

Utilizando-se da Figura 4-24, serão normalizados os termos e conceitos existentes no modelo de Análise de Riscos atualmente existente para Contratações de Tecnologia da Informação. A seguir serão listados os conceitos. Os termos foram extraídos da Figura 2-11.

1. Risco identificado;
2. Dano;
3. Impacto;
4. Responsável;

5. Probabilidade;
6. Ação preventiva e de contingência.

Após listados os conceitos, será feito o ‘de-para’ de cada item listado conforme definido no escopo inicial do trabalho, utilizando o conteúdo da proposto na ANBT NBR ISO 73.

### 4.2.1 Risco

A norma define risco como “um efeito e um desvio em relação ao esperado-positivo e/ou negativo”. Além deste conceito, são considerados os seguintes:

- Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar–se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).
- O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências ou uma combinação destes.
- O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade de ocorrência associada.
- A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

### 4.2.2 Dano

Não foi encontrada a definição de DANO na norma, o que torna inviável sua harmonização. A norma se refere a PERIGO, como sendo a fonte de um potencial dano. O perigo pode ser uma fonte de risco.

### 4.2.3 Impacto

A GR considera que fatores-chave e as tendências que tenham impacto sobre os objetivos da organização, é um termo de estabelecimento de contexto, especificamente de contexto externo. Em toda norma esse foi o único momento que a palavra impacto foi apresentada, o que também impede sua harmonização.

### 4.2.4 Responsável

A GR considera responsável como parte interessada a pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade. Um tomador de decisão pode ser uma parte interessada.

### 4.2.5 Probabilidade

A GR define probabilidade (*likelihood*) como chance de algo acontecer. Na terminologia de gestão de riscos, a palavra ”probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se de forma definida, medida ou determinada ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos ou freqüência, durante um determinado período de tempo.

Outra definição de probabilidade é o termo em Inglês "*likelihood*" que não têm um equivalente direto em algumas línguas; em vez disso, o equivalente do termo "*probability*" é frequentemente utilizado. Entretanto, em Inglês, "*probability*" é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos, ”*likelihood*" é utilizado com a mesma ampla interpretação de que o termo "*probability*" tem em muitos outros idiomas além do Inglês.

### 4.2.6 Ação preventiva e de contingência

Não citado na GR da GUIA 73, é também um conceito que não pode ser harmonizado de acordo com a GUIA 73.

### 4.2.7 Outros termos de gestão de riscos para a harmonização terminológica

A seguir, outros termos que podem ser considerados para uso na Gestão de Riscos.

#### 4.2.7.1 Gestão de riscos

Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

#### 4.2.7.2 Estrutura da gestão de riscos

Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização.

NOTA 1- Os fundamentos incluem a política, objetivos, mandatos e comprometimento para gerenciar riscos.

NOTA 2 Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades.

NOTA 3 A estrutura da gestão de riscos está incorporada no âmbito das políticas e práticas estratégicas e operacionais de toda a organização.

4.2.7.3 Política de gestão de riscos

Declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

4.2.7.4 Plano de gestão de riscos

Esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.

NOTA 1 - Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequência e a cronologia das atividades.

NOTA 2 - O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

4.2.7.5 Processo de gestão de riscos

Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos

4.2.7.6 Comunicação e consulta

Processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos .

NOTA 1 - As informações podem referir-se à existência, natureza, forma, probabilidade (*likelihood*), severidade, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos.

NOTA 2 A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou direcionar uma questão específica. A consulta é um processo que impacta uma decisão através da influência ao invés do poder; e uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.

4.2.7.7 Parte interessada

Pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade.

NOTA - Um tomador de decisão pode ser uma parte interessada.

4.2.7.8 Percepção do risco

Visão de risco da parte interessada.

NOTA - A percepção de risco reflete as necessidades, questões, conhecimento, crença e valores da parte interessada.

4.2.7.9 Estabelecimento do contexto

Definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos.

4.2.7.10 Contexto externo

Ambiente externo no qual a organização busca atingir seus objetivos.

NOTA - O contexto externo pode incluir:

O ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local.

Os fatores-chave e as tendências que tenham impacto sobre os objetivos da organização; e as relações com partes interessadas externas e suas percepções e valores.

4.2.7.11 Contexto interno

Ambiente interno no qual a organização busca atingir seus objetivos.

NOTA - O contexto interno pode incluir: governança, estrutura organizacional, funções e responsabilidades; políticas, objetivos e estratégias implementadas para atingi-los; capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias); sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais); relações com partes interessadas internas, e suas percepções e valores.

4.2.7.12 Cultura da organização

Normas, diretrizes e modelos adotados pela organização; e forma e extensão das relações contratuais.

4.2.7.13 Critérios de risco

Termos de referência contra os quais a significância de um risco é avaliada.

NOTA 1- Os critérios de risco são baseados nos objetivos organizacionais e no contexto externo e contexto interno.

NOTA 2- Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

4.2.7.14 Processo de avaliação de riscos

Processo global de identificação de riscos, análise de riscos e avaliação de riscos.

Termos relativos à identificação de riscos, processo de busca, reconhecimento e descrição de riscos.

NOTA 1- A identificação de riscos envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.

NOTA 2- A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

4.2.7.15 Descrição dos riscos

Declaração estruturada de riscos, contendo normalmente quatro elementos: fontes, eventos, causas e consequências.

4.2.7.16 Fonte de risco

Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

NOTA- Uma fonte de risco pode ser tangível ou intangível.

4.2.7.17 Evento

Ocorrência ou mudança em um conjunto específico de circunstâncias.

NOTA 1 - Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas.

NOTA 2 - Um evento pode consistir em alguma coisa não acontecer.

NOTA 3 - Um evento pode algumas vezes ser referido como um "incidente" ou um "acidente".

NOTA 4 Um evento sem consequências também pode ser referido como um "quase acidente", ou um "incidente" ou "por um triz".

4.2.7.18 Perigo

Fonte de potencial dano.

NOTA - O perigo pode ser uma fonte de risco.

4.2.7.19 Proprietário do risco

Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco

4.2.7.20 Análise de Riscos

Processo de compreender a natureza do risco e determinar o nível de risco

NOTA 1 - A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos

NOTA 2 - A análise de riscos inclui a estimativa de riscos.

4.2.7.21 Exposição

Grau em que uma organização e/ou parte interessada está sujeita a um evento.

#### 4.2.7.22 Consequência

Resultado de um evento que afeta os objetivos.

NOTA 1- Um evento pode levar a uma série de consequências.

NOTA 2- Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.

NOTA 3- As consequências podem ser expressas qualitativa ou quantitativamente.

NOTA 4- As consequências iniciais podem desencadear reações em cadeia

#### 4.2.7.23 Probabilidade

Medida da chance de ocorrência expressa como um número entre 0 e 1, onde 0 é a impossibilidade e 1 é a certeza absoluta.

#### 4.2.7.24 Frequência

Número de eventos ou resultados por unidade de tempo definida.

NOTA1- Frequência pode ser aplicada a eventos passados ou a potenciais eventos futuros, onde eles podem ser usados como uma medida de probabilidade (*likelihood*) probabilidade

#### 4.2.7.25 Vulnerabilidade

Propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência.

#### 4.2.7.26 Matriz de risco

Ferramenta para classificar e apresentar riscos definindo faixas para consequência e probabilidade (*likelihood*).

#### 4.2.7.27 Nível de risco

Magnitude de um risco expressa em termos da combinação das consequências e de suas probabilidades (*likelihood*).

4.2.7.28 Avaliação de riscos

Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

NOTA - A avaliação de riscos auxilia na decisão sobre o tratamento de riscos

4.2.7.29 Atitude perante o risco

Abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do risco.

4.2.7.30 Apetite pelo risco

Quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir.

4.2.7.31 Tolerância ao risco

Disposição da organização ou parte interessada em suportar o risco após o tratamento do risco a fim de atingir seus objetivos.

NOTA - A tolerância ao risco pode ser influenciada por requisitos legais ou regulatórios.

4.2.7.32 Aversão ao risco

Atitude de afastar-se de riscos.

4.2.7.33 Agregação de risco

Combinação de um número de riscos dentro de um único risco para desenvolver o mais completo entendimento do risco global.

4.2.7.34 Aceitação do risco

Decisão consciente de assumir um risco específico.

NOTA 1- A aceitação do risco pode ocorrer sem o tratamento do risco ou durante o processo de tratamento de riscos.

NOTA 2- Riscos aceitos estão sujeitos a monitoramento e análise crítica.

4.2.7.35 Tratamento de riscos

Processo para modificar o risco.

NOTA 1- O tratamento de risco pode envolver:

- A ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco.

- Assumir ou aumentar o risco, a fim de buscar uma oportunidade; a remoção da fonte de risco; a alteração da probabilidade (*likelihood*); a alteração das consequências; o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e a retenção do risco por uma escolha consciente.

NOTA 2- Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos".

NOTA 3- O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

4.2.7.36 Controle

Medida que está modificando o risco.

NOTA 1- Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco.

NOTA 2- Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

4.2.7.37 Ação de evitar o risco

Decisão informada de não se envolver, ou retirar-se de uma atividade, a fim de não ser exposto a um risco específico.

NOTA- A ação de evitar o risco pode ser baseada nos resultados da avaliação de riscos e/ou em obrigações legais e regulatórios.

4.2.7.38 Compartilhamento de riscos

Forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes.

NOTA 1- Requisitos legais ou regulatórios podem limitar, proibir ou ordenar o compartilhamento de risco.

NOTA 2- O compartilhamento de risco pode ser realizado através de seguros ou outras formas de contrato.

NOTA 3- A extensão em que o risco é distribuído pode depender da confiabilidade e clareza dos acordos de compartilhamento.

NOTA 4- A transferência de risco é uma forma de compartilhamento de risco.

4.2.7.39 Financiamento de riscos

Forma de tratamento de riscos que envolve arranjos contingentes para a provisão de fundos, a fim de atender ou modificar eventuais consequências financeiras, caso ocorram.

4.2.7.40 Retenção de riscos

Aceitação do benefício potencial de ganho, ou do ônus da perda, a partir de um risco específico.

NOTA 1- A retenção de riscos inclui a aceitação de riscos residuais.

NOTA 2- O nível de risco retido pode depender dos critérios de risco.

4.2.7.41 Risco residual

Risco remanescente após o tratamento do risco.

NOTA 1- O risco residual pode conter riscos não identificados.

NOTA 2- O risco residual também pode ser conhecido como "risco retido".

4.2.7.42 Resiliência

Capacidade adaptativa de uma organização em um ambiente complexo e de mudanças.

4.2.7.43 Monitoramento

Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

NOTA- O monitoramento pode ser aplicado à estrutura da gestão de riscos ao processo de gestão de riscos ao risco ou aos controles.

4.2.7.44 Análise crítica

Atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos.

NOTA- A análise crítica pode ser aplicada à estrutura da gestão de riscos ao processo de gestão de riscos ao risco ou aos controles.

4.2.7.45 Reporte de riscos

Forma de comunicação destinada a informar partes interessadas específicas, internas ou externas, fornecendo informações relativas ao estado atual do risco e a sua gestão

4.2.7.46 Registro de riscos

Registro de informações sobre riscos identificados.

NOTA- O termo "*risk log*" é algumas vezes utilizado no lugar de "registro de risco".

4.2.7.47 Perfil de risco

Descrição de um conjunto qualquer de riscos.

NOTA- O conjunto de riscos pode conter riscos que dizem respeito a toda a organização, parte da organização, ou referente ao qual tiver sido definido.

4.2.7.48 Auditoria de gestão de riscos

Processo sistemático, independente e documentado para obter evidências e avaliá-las de maneira objetiva, a fim de determinar a extensão na qual a estrutura da gestão de riscos ou qualquer parte sua selecionada, é adequada e efetiva.

### 4.2.8 Uso de outros termos nas contratações de TI

Muitos dos termos acima citados já são utilizados nas contratações de TI, entretanto, pode haver distorções no entendimento. A harmonização terminológica proposta neste trabalho, poderá dirimir dúvidas e evitar o uso incorreto de conceitos de gestão de riscos utilizados nas contratações de TI.

## 4.3 A PROPOSTA DO ARTEFATO PARA IDENTIFICAÇÃO DE RISCOS NAS CONTRATAÇÕES DE TI

Para escolha dos conceitos foi adotado o critério de seleção dos itens que estavam presentes nas referências pesquisadas e que abordaram identificação de riscos. Eles refletem as ideias apresentadas nos mapas mentais. No artefato, as informações foram otimizadas de modo a não repetir os itens que já foram contemplados nos documentos Análise de Viabilidade, Plano de Sustentação e Estratégia da Contratação, tornando o artefato para Identificação de Riscos uma atividade complementar ao processo atualmente existente.

Com essas informações será proposto o artefato detalhado da atividade de Identificação de Riscos. Conforme preconiza a ABNT NBR ISO 31000, a Identificação de Riscos deve anteceder a Análise de Riscos (ABNT, 2009a). Os itens que compõem a proposta foram devidamente ajustados para um novo molde. Ou seja, as ideias que estavam em forma de conceito (1º nível) ou atividade (2º nível) foram adaptadas e niveladas para que o artefato pudesse utilizar informações apenas de conceitos (1º nível), o que o mantém com o direcionador de ser mais abrangente por ser a primeira proposta. Há, portanto, devido a este nivelamento, pequenas adaptações semânticas nos conceitos encontrados, mas que não alteram a ideia original dos autores, normas ou modelos.

Os itens do artefato podem ser usados para dar aos gestores de TI mais opções no que se refere ao cenário para encontrar os riscos, promovendo a reflexão e a discussão de riscos não previstos. A Tabela 4-1 apresenta o artefato de Identificação de Riscos, com as devidas fontes de onde foram extraídos os conceitos. Os que possuírem "*" no final foram adaptados e nivelados semanticamente.

**Tabela 4-1** Proposta de artefato para Identificação de Riscos nas contratações de TI

| **Proposta de Artefato para Identificação de Riscos nas Contratações de TI** | | |
|---|---|---|
| O usuário deste artefato deve avaliar se existem riscos referentes às premissas apresentadas, que de alguma forma possam comprometer o sucesso da contratação.<br><br>Cada item encontrado deve ser listado no documento de Análise de Riscos, para a devida classificação, priorização e tratamento de cada risco. Os riscos devem ser revistos e avaliados durante toda a contratação se necessário. | | |
| **Etapa 1 - Estabelecimento do Contexto** | **Contexto interno da contratação** | **NBR ABNT ISO 31000** |
| | Governança | |
| | Estrutura organizacional | |
| | Funções e responsabilidades | |
| | Políticas, objetivos e estratégias | |
| | Partes interessadas (percepções e valores)* | |
| | Normas, diretrizes e modelos da organização* | |
| | Recursos Financeiros * | |
| | Tempo | |
| | Pessoas (recursos humanos)* | |
| | Processo de negócio* | |
| | Sistemas e tecnologias correlatos (interno)* | |
| | Relações contratuais* | |
| | **Contexto externo da contratação** | |
| | Social | |
| | Político | |
| | Legal (Jurídico)* | |
| | Regulatório | |
| | Sistemas e tecnologias correlatos (externo)* | |
| | Natural (ambientais)* | |
| | Competitivo/Comercial/Mercado (negócio)* | |
| | Contexto Local/ Regional/ Nacional/ Internacional * | |
| **Etapa 2 - Riscos do Processo** | Competências de relacionamento entre clientes e fornecedores | **Cruz; et al. (2011)** |
| | Competências administrativas e jurídicas | |
| | Histórico de eventos danosos em licitações | |
| | Possíveis problemas na licitação (consultar pregoeiro)* | |

| | | |
|---|---|---|
| | Histórico de eventos danosos em contratações do mesmo tipo (outros órgãos)* | |
| | Riscos pessoais do servidor | **Motta (2010)** |
| | Treinamentos insuficientes do servidor | |
| | Forte pressão dos escalões | |
| | Inexistentes incentivos salariais pelo desempenho do servidor | |
| | Ética do servidor | |
| **Etapa 3 - Riscos da Solução** | Requisitos técnicos* | **PMI (2004)** |
| | Desempenho e confiabilidade | |
| | Qualidade | |
| | Subcontratadas e fornecedores | |
| | Clientes (interno e externo)* | |
| **Etapa 4 - Riscos de Projeto (Gerais)** | Escopo | **PMI (2004)** |
| | Tempo | |
| | Custo | |
| | Dependências do Projeto | |
| | Recursos | |
| | Financiamento | |
| | Priorização | |
| | Estimativa | |
| | Planejamento | |
| | Comunicação | |
| **Etapa 5 - Riscos de Projeto (Específicos)** | Descontinuidade tecnológica | **Cruz (2008)** |
| | Dependência do fornecedor | |
| | Definição do escopo dos serviços* | |
| | Não compreensão do negócio pelos contratados* | |
| | Manter a qualidade dos serviços* | |
| | Perda do domínio do conhecimento de negócio | |
| | Perda do controle da informação de negócio (troca de profissionais)* | |
| | Perda de política interna de incentivo aos servidores (ou inexistente)* | |
| | Disputas entre equipes internas e de terceiros | |
| | Problemas com diferenças de rendimentos (contratada)* | |

| | | |
|---|---|---|
| | Segurança das informações de negócio | |
| | Desequilíbrio financeiro do contrato | |
| | Perda de controle dos custos do contrato | |
| | Impugnação da licitação ou suspensão da assinatura do contrato* | |
| | Suspensão ou rompimento de contratos considerados ilegais | |
| | Perdas orçamentárias* | |
| | Paralisação de projetos importantes calcados em TI | |
| | Ressarcimento, pelos gestores, de prejuízos quantificados* | |
| | Responder um processo criminal* | |
| | Quantidade e a qualificação do pessoal disponível* | |
| | Motivação das pessoas envolvidas* | |
| | Riscos relacionados com a governança das contratações | |
| | Aumento do prazo para contratação* | |
| | Aumento do custo burocrático* | |
| | Resistências das pessoas (inércia, motivações pessoais ou preconceitos) | |
| | Obstáculos organizacionais (burocracia, falta de planejamento etc.) | |
| | Falta de conhecimento básico sobre contratações* | |
| | Falta de conhecimento jurídico especializado disponível* | |
| | Governança corporativa (carência de alinhamento dos *stakeholders*) | |
| | Desalinhamento estratégico* | |
| | Necessidade de envolvimento de áreas muito distintas | |
| | Contextos não adequadamente compartilhados entre as áreas envolvidas | |
| | Padronização e execução de processos mais rigorosos | |
| | Interface com atores externos (clientes e fornecedores internos e externos) | |
| | Obstáculos devidos a interesses escusos (corrupção) | |
| | Falta de integração entre as áreas | |
| | Falta de compartilhar contextos e experiências* | |
| | Existência de falhas de comunicação e conflitos mudos* | |
| | Falta de uma linguagem comum (jurídica x tecnologia) | |
| | Falta de conhecimento da legislação | |
| | Falta de qualificação das pessoas | |

| | | |
|---|---|---|
| | Falta de pessoas em número suficiente | |
| | Existência de fatores pessoais (vaidade, competição, medo) | |
| | Falta de visão sistêmica do processo | |
| | Falta de formalização do processo de contratação | |
| | Falhas na execução do processo | |
| | Deficiências na gestão (rotativo de líderes; deficiência no planejamento) | |
| | Falhas na organização (foco na estrutura; sem área de contratos)* | |
| | Sobrecarga de trabalho | |
| | Indefinição de papéis e responsabilidades, (problemas de comunicação)* | |

Para simplificar a aplicação do artefato, foi gerada uma versão para coleta de dados. A Tabela 4-2 apresenta a versão que será aplicada.

**Tabela 4-2** Proposta de artefato para Identificação de Riscos nas contratações de TI (aplicado).

| ID | Etapa 1 - Contexto interno da contratação | Descreva os riscos que estão associados |
|---|---|---|
| 1 | Governança | |
| 2 | Estrutura organizacional | |
| 3 | Funções e responsabilidades | |
| 4 | Políticas, objetivos e estratégias | |
| 5 | Partes interessadas (percepções e valores) | |
| 6 | Normas, diretrizes e modelos da organização | |
| 7 | Recursos Financeiros | |
| 8 | Tempo | |
| 9 | Pessoas (recursos humanos) | |
| 10 | Processo de negócio | |
| 11 | Sistemas e tecnologias correlatos (interno) | |
| 12 | Relações contratuais | |
| | **Contexto externo da contratação** | |
| 13 | Social | |
| 14 | Político | |
| 15 | Legal (Jurídico) | |
| 16 | Regulatório | |
| 17 | Sistemas e tecnologias correlatos (externo) | |
| 18 | Natural (ambientais) | |
| 19 | Competitivo/Comercial/Mercado (negócio) | |
| 20 | Contexto Local/ Regional/ Nacional/ Internacional | |

| | | |
|---|---|---|
| | **Etapa 2 - Riscos do Processo** | |
| 21 | Competências de relacionamento entre clientes e fornecedores | |
| 22 | Competências administrativas e jurídicas | |
| 23 | Histórico de eventos danosos em licitações | |
| 24 | Possíveis problemas na licitação (consultar pregoeiro) | |
| 25 | Histórico de eventos danosos em contratações do mesmo tipo (outros órgãos) | |
| 26 | Riscos pessoais do servidor | |
| 27 | Treinamentos insuficientes do servidor | |
| 28 | Forte pressão dos escalões | |
| 29 | Inexistentes incentivos salariais pelo desempenho do servidor | |
| 30 | Ética do servidor | |
| | **Etapa 3 - Riscos da Solução** | |
| 31 | Requisitos técnicos | |
| 32 | Desempenho e confiabilidade | |
| 33 | Qualidade | |
| 34 | Subcontratadas e fornecedores | |
| 35 | Clientes (interno e externo) | |
| | **Etapa 4 - Riscos de Projeto (Gerais)** | |
| 36 | Escopo | |
| 37 | Tempo | |
| 38 | Custo | |
| 39 | Dependências do Projeto | |
| 40 | Recursos | |
| 41 | Financiamento | |
| 42 | Priorização | |
| 43 | Estimativa | |
| 44 | Planejamento | |
| 45 | Comunicação | |
| | **Etapa 5 - Riscos de Projeto (Específicos)** | |
| 46 | Descontinuidade tecnológica | |
| 47 | Dependência do fornecedor | |
| 48 | Definição do escopo dos serviços | |
| 49 | Não compreensão do negócio pelos contratados | |
| 50 | Manter a qualidade dos serviços | |
| 51 | Perda do domínio do conhecimento de negócio | |
| 52 | Perda do controle da informação de negócio (troca de profissionais) | |
| 53 | Perda de política interna de incentivo aos servidores (ou inexistente) | |
| 54 | Disputas entre equipes internas e de | |

| | | |
|---|---|---|
| | terceiros | |
| 55 | Problemas com diferenças de rendimentos (contratada) | |
| 56 | Segurança das informações de negócio | |
| 57 | Desequilíbrio financeiro do contrato | |
| 58 | Perda de controle dos custos do contrato | |
| 59 | Impugnação da licitação ou suspensão da assinatura do contrato | |
| 60 | Suspensão ou rompimento de contratos considerados ilegais | |
| 61 | Perdas orçamentárias | |
| 62 | Paralisação de projetos importantes calcados em TI | |
| 63 | Ressarcimento, pelos gestores, de prejuízos quantificados | |
| 64 | Responder um processo criminal | |
| 65 | Quantidade e a qualificação do pessoal disponível | |
| 66 | Motivação das pessoas envolvidas | |
| 67 | Riscos relacionados com a governança das contratações | |
| 68 | Aumento do prazo para contratação | |
| 69 | Aumento do custo burocrático | |
| 70 | Resistências das pessoas (inércia, motivações pessoais ou preconceitos) | |
| 71 | Obstáculos organizacionais (burocracia, falta de planejamento etc.) | |
| 72 | Falta de Conhecimento básico sobre contratações | |
| 73 | Falta de Conhecimento jurídico especializado disponível | |
| 74 | Governança corporativa (carência de alinhamento dos *stakeholders*) | |
| 75 | Desalinhamento estratégico | |
| 76 | Necessidade de envolvimento de áreas muito distintas | |
| 77 | Contextos não adequadamente compartilhados entre as áreas envolvidas | |
| 78 | Padronização e execução de processos mais rigorosos | |
| 79 | Interface com atores externos (clientes e fornecedores internos e externos) | |
| 80 | Obstáculos devidos a interesses escusos (corrupção) | |
| 81 | Falta de integração entre as áreas | |
| 82 | Falta de compartilhar contextos e experiências | |
| 83 | Existência de falhas de comunicação e conflitos mudos | |
| 84 | Falta de uma linguagem comum (jurídica x tecnologia) | |
| 85 | Falta de conhecimento da legislação | |

| | | |
|---|---|---|
| 86 | Falta de qualificação das pessoas | |
| 87 | Falta de pessoas em número suficiente | |
| 88 | Existência de fatores pessoais (vaidade, competição, medo) | |
| 89 | Falta de visão sistêmica do processo | |
| 90 | Falta de formalização do processo de contratação | |
| 91 | Falhas na execução do processo | |
| 92 | Deficiências na gestão (rotativo de líderes; deficiência no planejamento) | |
| 93 | Falhas na organização (foco na estrutura; sem área de contratos) | |
| 94 | Sobrecarga de trabalho | |
| 95 | Indefinição de papéis e responsabilidades, (problemas de comunicação) | |

Nesta proposta de artefato que especifica a Identificação de Riscos nas contratações de TI, destacam-se em sua composição cinco fases que foram apresentadas na Tabela 4-1 e 4-2:

- Etapa 1 - Estabelecimento do contexto para identificar riscos;
- Etapa 2 - Riscos do Processo;
- Etapa 3 - Riscos da Solução;
- Etapa 4 - Riscos do Projeto (Gerais);
- Etapa 5 - Riscos do Projeto (Específicos).

Esta classificação permite que o artefato seja utilizado com um enfoque abrangente que permite encontrar o nível de detalhamento mais apropriado para cada contratação, ampliando as possibilidades de identificação de riscos em relação à maneira atual, utilizando conceitos provenientes da ABNT NBR ISO 31000.

É importante destacar que este artefato é um *template* genérico que poderá ser utilizado para apoio na identificação de riscos nas contratações de TI. Cada contratação, cada objeto, cada órgão possui particularidades, processos, políticas, valores e pessoas que devem ser consideradas. Por isso o artefato não tem a intenção de ser o único referencial para essa questão. O principal desafio deste artefato será traduzir um processo intuitivo de "tentar encontrar" riscos para um mapeamento formal de atividades e conceitos, que centralizados poderão ajudar na percepção para se construir uma identificação de riscos mais completa.

Para atingir o objetivo científico de validação do modelo proposto foram realizadas duas validações do artefato. Uma analítica e outra prática, por meio de um estudo de caso. O Capítulo 5 apresenta as validações.

# 5. ESTUDO DE CASO

## 5.1 ESTUDO DE CASO

Para que se analise e avalie o comportamento do artefato de Identificação de Riscos foi realizada uma aplicação prática, por meio de um estudo de caso. Essa aplicação envolve uma contratação real que aconteceu em uma organização pública, no âmbito do SISP.

A identidade da organização pública será preservada pelo fato de o representante máximo de TI da instituição julgar que, ao revelar seu nome, estaria divulgando uma informação que poderia expor a organização. Por este motivo, não será divulgada a identidade do órgão envolvido na aplicação prática. Ela será referenciada como "Organização Pública".

A Organização Pública tem experiência em elaborar contratações e possui significativo orçamento para contratações de TI no âmbito do Governo Federal. A organização aceitou fazer parte deste estudo de caso, por estar buscando melhorias que ampliem o conhecimento organizacional nessa atividade.

A proposta do artefato de Identificação de Riscos a ser utilizado, envolveu o levantamento do estado da arte de normas de riscos e subsidiou a elaboração do questionário para a pesquisa de campo.

O levantamento de dados ocorreu por meio da entrega e coleta de formulários impressos diretamente no escritório ou em local previamente combinado dos respondentes, que deveriam ter como premissa, ter planejado ao menos uma contratação com todos os artefatos da contratação (incluindo Análise de Riscos) entre 2010 e 2012.

A escolha deste método foi feita devido ao critério adotado por Castro (2010) que percebeu que a estratégia de ir pessoalmente aos respondentes tem um índice de retorno de 70%. O uso de questionários *online*, ou por *e-mail*, tem taxa de retorno de apenas 30%.

Em relação à contratação foi escolhido um planejamento da contratação realizado após o ano de 2010, especificamente de suporte em sistemas de informação. A escolha desta contratação foi dada aleatoriamente, uma vez que existiam diversas outras que poderiam ser escolhidas nesta Organização Pública. Os detalhes desta contratação não serão revelados, uma vez que uma simples busca pela internet poderia resultar numa inferência de qual organização realizou a contratação. Como os artefatos de planejamento da

contratação, incluindo o objeto de estudo que é a analise de riscos não ficam disponibilizadas no edital, registra-se que a busca deste documento foi feita por meio da pesquisa no próprio processo de contratação, onde foi necessário pesquisar "*in loco*" no arquivo da Organização Pública em questão.

### 5.1.1 Etapas do estudo de caso

Foram adotadas as seguintes etapas para coleta de dados:

- Identificação do perfil dos servidores que confeccionaram os artefatos da contratação;
- Definição do universo da pesquisa;
- Plano amostral;
- Coleta de dados;
- Aplicação do artefato de Identificação de Riscos;
- Resultados e comparações.

### 5.1.2 Perfil dos servidores

Antes da coleta de dados foi levantado qual o perfil da equipe de planejamento da contratação que confeccionou o artefato, com base nas informações disponibilizadas no planejamento da contratação. A estrutura foi adaptada do formulário apresentado por Castro (2010). Foram realizadas as seguintes perguntas aos entrevistados:

- Idade (anos);
- Experiência com contratação de TI (em anos);
- De quantas contratações participou entre 2010 e 2012?
- Possui curso de formação de gestores de TI (módulo Planejamento da Contratação)?
- Existe algum outro servidor que atua em parceria nas contratações ou o trabalho de se identificar riscos é realizado individualmente?
- Existe algum referencial teórico adicional que é aplicado para se identificar os riscos da contratação?

A aplicação do questionário aos dois servidores que participaram do planejamento da contratação da licitação em questão resultou na Tabela 5-1.

**Tabela 5-1** - Perfil da Equipe de Planejamento da Contratação.

| Critério | Resposta |
|---|---|
| Média de Idade (anos) | 53 |
| Experiência com contratação de TI (anos) | 25 |
| De quantas contratações participou entre 2010 e 2012? | 30 |
| Possui curso de formação de gestores de TI (módulo Planejamento da Contratação)? | Não |
| Existe algum outro servidor que atua em parceria nas contratações ou o trabalho de se identificar riscos é realizado individualmente? | Sim |
| Existe algum referencial teórico adicional que é aplicado para se identificar os riscos da contratação? | Não |

### 5.1.3 Plano Amostral

A amostra foi formada a partir dos artefatos preenchidos pelos respondentes da contratação selecionada, que já haviam preenchido os riscos identificados, quando da contratação realizada. Com o novo artefato, eles tiveram uma nova oportunidade de rever os possíveis riscos que poderiam afetar a contratação.

### 5.1.4 Universo da Pesquisa

O universo da pesquisa foi formado por respondentes de Brasília, da Esplanada dos Ministérios, de um dos órgãos do SISP, que atuam com contratações de TI.

### 5.1.5 Coleta de dados

A coleta de dados se deu através da extração dos riscos identificados por estes servidores na contratação selecionada, no documento "Análise de Riscos". A compilação das informações resultou na Tabela 5-2**.**

**Tabela 5-2** - Riscos coletados da Análise de Riscos da contratação.

| **RISCOS DO PROCESSO DE CONTRATAÇÃO** | |
|---|---|
| **N** | **Risco** |
| 1 | Atraso no processo de contratação |
| 2 | Alteração do escopo do objeto contratado ou aumento das necessidades de serviços |
| 3 | Rotatividade da equipe de Planejamento da contratação |
| 4 | Atraso na entrega do Plano de Ação |
| 5 | Atraso na execução do Plano de Ação |
| **RISCOS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO** | |
| **N** | **Risco** |
| 6 | Atraso na execução do Plano de Ação |

Com estas informações, a viabilidade de aplicar o artefato construído neste trabalho se torna real, para a verificação dos resultados que podem vir a ser apresentados.

### 5.1.6 Aplicação do artefato de Identificação de Riscos

Para aplicação do artefato de identificação de risco foi estudada a contratação selecionada aleatoriamente, conforme descrito em 5.2, para que sejam identificados outros riscos que possam trazer impactos no decorrer do processo. Ou seja, além dos riscos já identificados com o artefato atualmente existente, quais seriam os que iriam ser percebidos com o novo artefato, proposto por este trabalho?

A mesma equipe de planejamento da contratação que elaborou a análise de riscos inicial analisou o artefato e marcou as opções que seriam importantes de serem consideradas, com apoio do novo artefato. Ao aplicar o artefato, foram identificados riscos adicionais aos apresentados na Tabela 5-2. Os novos riscos foram compilados na Tabela 5-3, e alguns tiveram comentários adicionais pelos gestores, que foram colocados entre parênteses e destacados com o símbolo #.

**Tabela 5-3** - Riscos encontrados com o novo artefato de Identificação de Riscos.

| N | ID | NOVOS RISCOS IDENTIFICADOS | Prioridade |
|---|---|---|---|
| **1** | 6 | Normas, diretrizes e modelos da organização (desatualizadas) # | 1 |
| **2** | 9 | Pessoas (RH) – (Falta de método para conduzir o processo) # | 16 |
| **3** | 10 | Processo de negócio (não mapeados) # | 2 |
| **4** | 14 | Político (interferências de decisões políticas sem ampla discussão) # | 3 |
| **5** | 20 | Contexto Local/ Regional/ Nacional/ Internacional* | 15 |
| **6** | 27 | Treinamentos insuficientes do servidor | 14 |
| **7** | 29 | Inexistentes incentivos salariais pelo desempenho do servidor | 13 |
| **8** | 31 | Requisitos técnicos (ausências de requisitos) # | 4 |
| **9** | 35 | Clientes (interno e externo)* (falta de Acordo de Serviço) # | 12 |
| **10** | 42 | Priorização (ausência de priorização das atividades da contratação) # | 0 |
| **11** | 45 | Comunicação (ausência de plano de comunicação) # | 5 |
| **12** | 50 | Manter a qualidade dos serviços (Ausência de estratégia de continuidade) | 11 |
| **13** | 51 | Perda do domínio do conhecimento de negócio (negligência da empresa) # | 10 |
| **14** | 52 | Perda do controle da informação de negócio (troca de profissionais) | 9 |
| **15** | 70 | Resistências das pessoas (inércia, motivações pessoais ou preconceitos) | 8 |
| **16** | 89 | Falta de visão sistêmica do processo | 6 |
| **17** | 94 | Sobrecarga de trabalho (do gestor) | 7 |

### 5.1.7 Resultados

A Tabela 5-2 que se refere aos riscos identificados pelos gestores com o artefato atualmente existente, apresentou apenas cinco riscos sob a ótica do processo de contratação. O primeiro risco, que trata do "Atraso no processo de contratação", possui associação com todas as atividades identificadas no novo artefato (1*N, sendo N=17, originado da Tabela 5-3), pois qualquer uma delas pode impactar em atraso no processo de contração. A propósito, a identificação deste risco por parte do gestor no primeiro artefato foi superficial, pois não especificou sob qual aspecto a contratação poderia atrasar. Já no artefato proposto é possível perceber um detalhamento maior nos conceitos encontrados, permitindo uma percepção de quais itens, de fato, o gestor deve ser preocupar.

O segundo risco "Alteração do escopo do objeto contratado ou aumento das necessidades de serviços" possui os seguintes itens relacionados:

1) Priorização (ausência de priorização das atividades da contratação)
2) Processo de negócio (não mapeados) #
3) Político (interferências de decisões políticas sem ampla discursão) #
4) Treinamentos insuficientes do servidor
5) Requisitos técnicos (ausências de requisitos) #
6) Clientes (interno e externo)* (falta de Acordo de Serviço) #

Ou seja, o risco encontrado inicialmente pelo formulário original, apresenta mais seis especificações e desdobramentos que foram percebidos com a aplicação do novo formulário.

O terceiro risco apontado pelo gestor "Rotatividade da equipe de Planejamento da Contratação", possui os seguintes riscos associados:

1) Pessoas (RH) - (Falta de método para conduzir o processo) #
2) Processo de negócio (não mapeados) #
3) Político (interferências de decisões políticas sem ampla discussão) #
4) Treinamentos insuficientes do servidor
5) Inexistentes incentivos salariais pelo desempenho do servidor
6) Comunicação (ausência de plano de comunicação) #
7) Perda do controle da informação de negócio (troca de profissionais)

8) Resistências das pessoas (inércia, motivações pessoais ou preconceitos)
9) Falta de visão sistêmica do processo
10) Sobrecarga de trabalho (do gestor).

Os riscos "Atraso na entrega do Plano de Ação" e "Atraso na execução do Plano de Ação" não tiveram associações com os novos riscos encontrados, porque não foi definido pelo gestor sobre o que se tratava o plano de ação em questão. Foi uma proposição aberta, que não permitiu a associação com outras atividades identificadas com o novo artefato.

Desta forma, foi gerada a Figura 5-1, que representa as associações encontradas no comparativo entre o formulário de identificação de riscos do Guia de Contratações do SISP e o proposto neste trabalho.

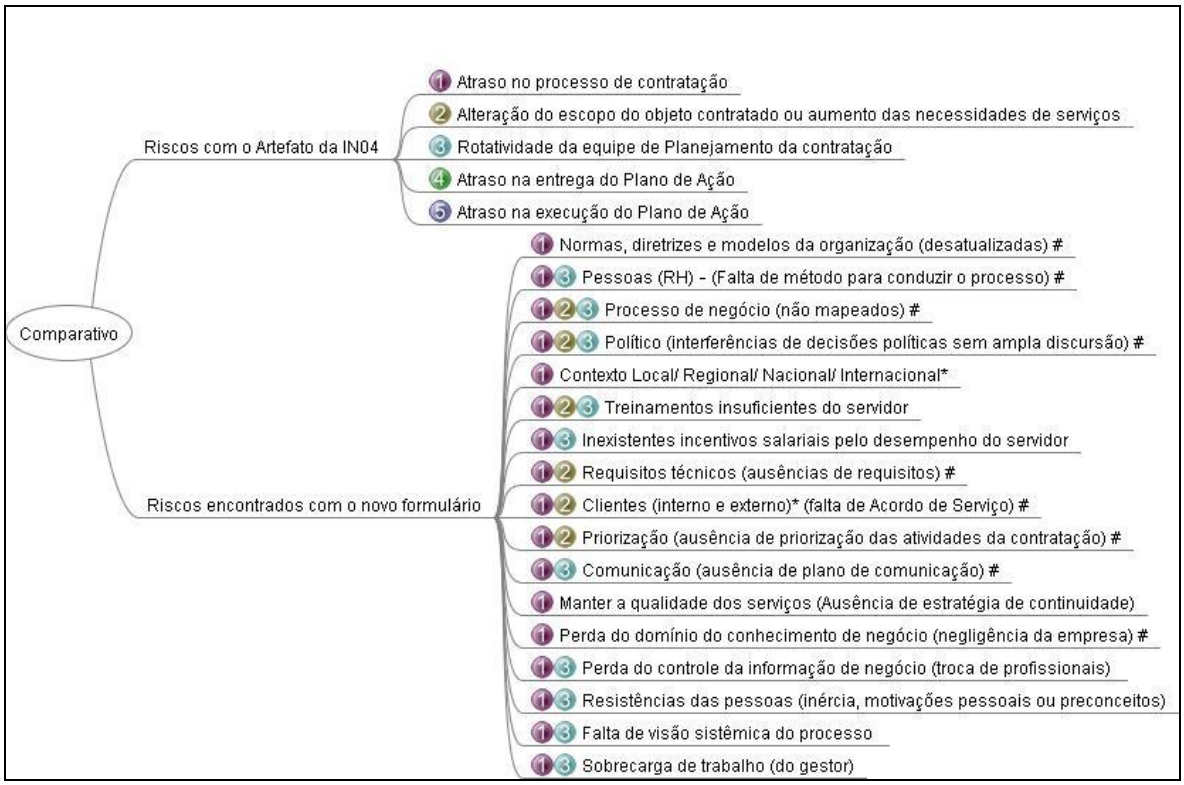


Figura 5-1- Associações de riscos encontrados com formulário atual x proposto.

A Figura 5-1 permite inferir que os seis riscos encontrados inicialmente, associados com os novos riscos percebidos com o novo formulário, permitem um detalhamento maior dos riscos encontrados. Os riscos que foram encontrados no novo formulário refletem uma preocupação adicional que o gestor deve ter para planejar a contratação em questão. O relacionamento de 1:N do antigo formulário em relação ao primeiro mostra que existe uma lacuna significativa para a identificação de riscos. A proposta do novo formulário torna

mais simples e compreensiva a atividade que pode estar sendo negligenciada por equipes de planejamento da contratação. Com o novo formulário, a criticidade desta atividade poderá ser observada com maior cuidado e rigor. Observa-se também que os riscos 4 e 5 encontrados pelo gestor no primeiro formulário, foram vagos e não ficaram claros para sequer serem comparados.

Outra preocupação é que a equipe de Planejamento da Contratação deste órgão foi composta na contratação selecionada, por apenas dois servidores. Ou seja, possivelmente um servidor assumiu dois papéis, dos três que devem compor os integrantes da equipe de planejamento da contratação, a saber: integrante técnico, requisitante e administrativo.

Adicionalmente, os dados levantados permitiram a percepção do quantitativo de riscos que foram observados pelos gestores da contratação em questão. A análise gerou a Figura 5-2.

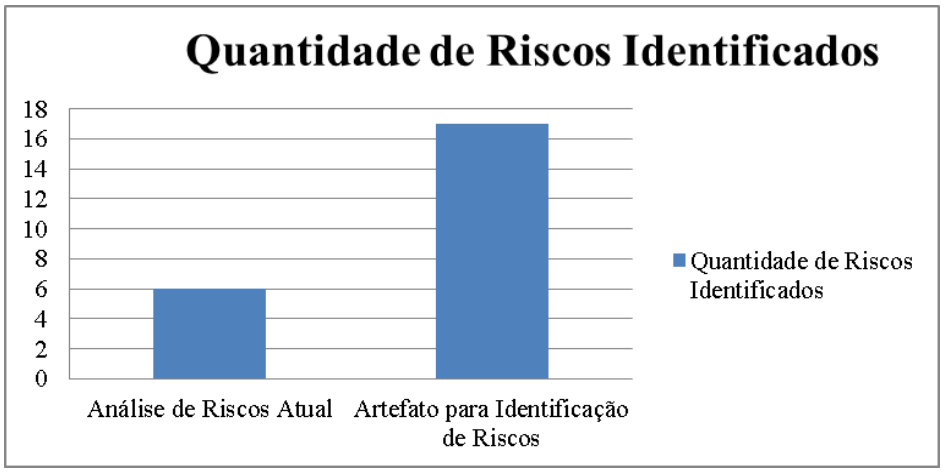


Figura 5-2 Quantidade de Riscos identificados pelo modelo atual x artefato proposto.

Com o método de identificação de riscos atual foram encontrados 6 (seis) riscos pelo gestor. No contexto da contratação em questão, com o uso do Artefato para Identificação de Riscos proposto neste trabalho, foram percebido adicionalmente mais 17 riscos, que podem estar relacionados aos riscos já identificados, porém com um nível maior de detalhamento.

Verifica-se portanto, que o novo artefato tem a capacidade de indicar ainda mais fatores que podem influenciar a contratação. Logo, os quantitativos totais de riscos dessa contratação executada em 2011, e novamente planejada sob a ótica do artefato proposto no presente trabalho no ano de 2012 apresentou o quantitativo destacado na Figura 5-3.

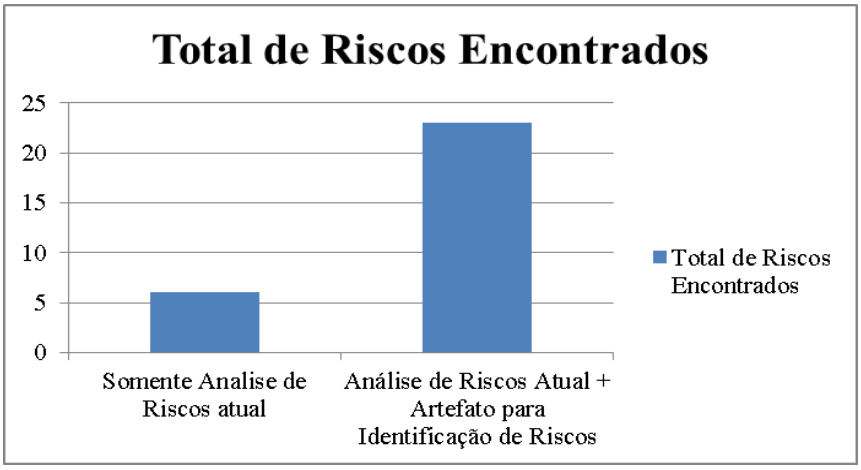


Figura 5-3 Total de riscos encontrados.

Com isso pode-se afirmar que o somatório dos riscos encontrados com o modelo atual + o artefato de Identificação de Riscos totaliza 23 riscos identificados, numa contratação que inicialmente havia identificado apenas 6 (seis) riscos.

Considerando a experiência da equipe de planejamento da contratação, bem como o quantitativo de contratações que participaram, além da média de idade dos servidores, verifica-se que os riscos adicionais não foram encontrados por falta de um conteúdo ou referencial teórico que direcione os servidores para uma percepção mais ampla na maneira de se identificar os riscos. A falta do curso de formação de gestores de TI (atualmente coordenado pela ENAP), pode também ter influenciado na baixa percepção de riscos identificados.

Fica evidente que a aplicação do artefato poderá apontar mais opções, contribuindo assim para uma visão mais crítica da etapa de identificação de riscos. Isso irá consequentemente melhorar o próprio processo da Análise de Riscos proposto pela IN04, pois após uma identificação mais detalhada será feito uma análise baseada em mais variáveis que deveriam ser consideradas e só puderam ser percebidas após a aplicação do artefato.

A Figura 5-4 apresenta a representação do cenário proposto com o presente trabalho para aprimorar o processo de análise de riscos com base na coleta de experiências de todas APF.

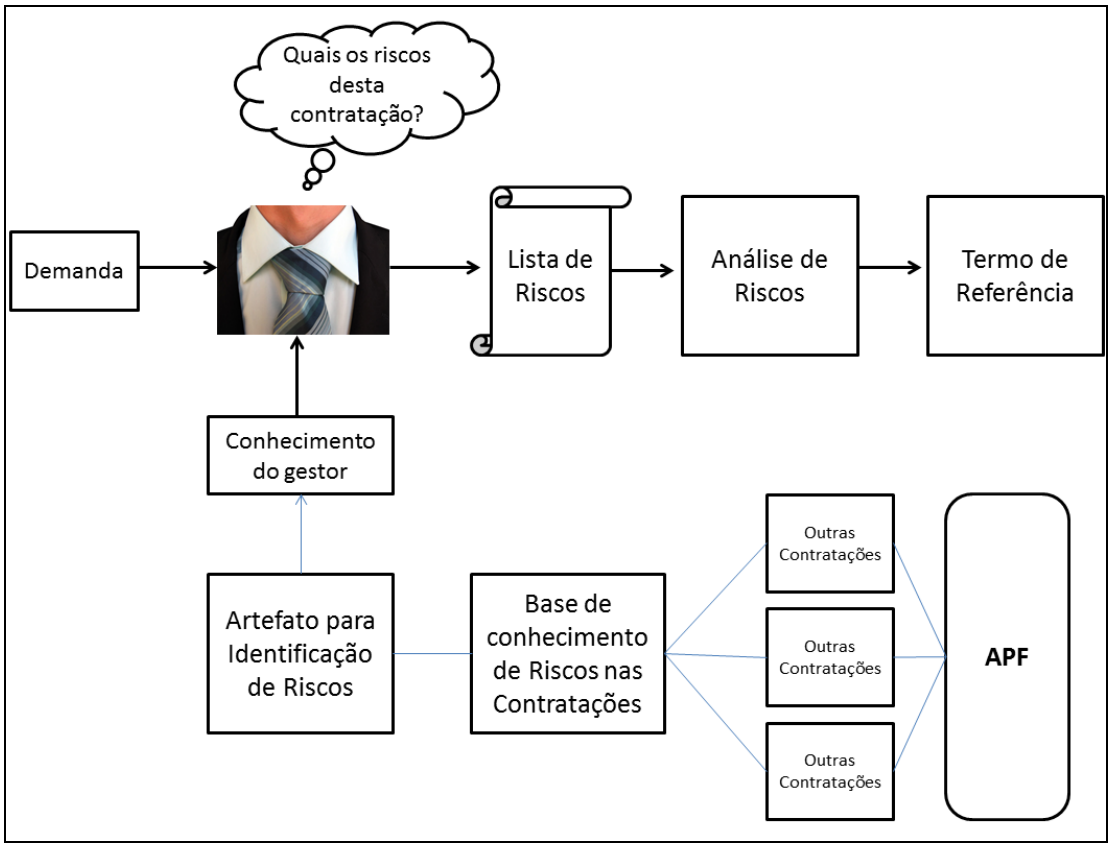


Figura 5-4 Aprimoramento da Análise de Riscos na APF.

Sob a ótica dos resultados encontrados com este trabalho é possível inferir que o estudo de caso permitiu observar que o novo formulário gera novas inclusões de riscos que devem ser devidamente tratados.

De acordo com os resultados encontrados é possível perceber também que o tempo de experiência e a idade dos membros da equipe de planejamento da contratação não significam necessariamente que os requisitos de identificação de riscos serão completamente atingidos.

# 6. CONCLUSÕES

A busca por um planejamento da contratação de uma solução de TI na APF aderente às leis e normas é uma preocupação natural dos gestores de TI, que buscam em suas especificações comprar o melhor bem ou serviço que atenda à demanda, aliado ao menor preço. Com a utilização da abordagem proposta pelo presente trabalho, as especificações poderão ser mais bem detalhadas, com a identificação de riscos de maneira mais transparente e metodologicamente mais adequada para a realidade das contratações de TI.

Essa mudança de paradigma na maneira de se identificar riscos pode se encaixar na realidade de vários órgãos, pois o foco do processo de entrega do termo de referência poderá ser ampliado com a abordagem sistemática aqui proposta, com o artefato de Identificação de Riscos.

Afinal, na situação anterior ao modelo proposto, os gestores tinham como diretriz uma instrução única que era permear todas as etapas do planejamento da contratação com a análise de riscos. Ou seja, caberia retirar de cada item dos artefatos de Análise de Viabilidade, Plano de Sustentação e Estratégia da Contratação, o que poderia ser elencado como riscos, para então analisá-los. Se o gestor não preenchesse as informações nas várias perspectivas na fase de planejamento da contratação, a compra certamente deixaria de considerar riscos em potencial, capazes de dificultar o sucesso da contratação por não estarem ao alcance de quem especifica. Nessa situação, o gestor nem imagina que alguns critérios ou conceitos devem ser considerados, simplesmente por desconhecer ou por não ter um material mínimo de referência para seguir, tal como foi proposto no artefato que contém itens de relevância não especificados nos artefatos que antecedem a Análise de Riscos.

Isso por que existe um hiato metodológico entre o documento de Análise de Riscos e as fases que o antecedem. Considerando a ausência de método, sob a ótica de identificação de riscos, para se gerar o termo de referência, há grande chance de ocorrer nos termos de referência ausência de itens de riscos, levando a consequentes falhas nas fases seguintes da contratação, especialmente na gestão contratual.

A utilização do artefato que corresponde a um detalhamento da atividade de identificação de riscos aqui proposto poderá resultar em uma identificação de riscos mais precisa e que permitirá uma gestão contratual com menos chances de ficar exposta a incidentes não

previstos. A ausência da exatidão na definição de conceitos deixa o gestor vulnerável, pois as falhas da contratação poderiam ser alvo de fornecedores intencionados em explorar vulnerabilidades. Por outro lado, os órgãos de controle podem entender que houve negligência por parte dos gestores de TI que especificaram o trabalho, por terem deixando de considerar fatores críticos, mas que por sua vez não foram considerados por falta de um referencial estabelecido para as contratações.

O processo de contratação, atualmente feito com a identificação dos riscos sem direcionadores práticos preestabelecidos, resulta numa heterogeneidade de itens de riscos para contratações de mesmo objeto, em órgãos diferentes, o que pode gerar visões diferentes para o mesmo conceito. Por exemplo, um órgão poderia pagar muito mais caro por um bem, simplesmente por que os termos de referência possuem especificações e cláusulas diferentes, baseadas em diferentes riscos identificados (foram feitos por pessoas diferentes, com visões diferentes). Considerando que boa parte das contratações de TI são de *commodities*, essa heterogeneidade deve ser evitada, por mais que cada órgão tenha particularidades, visto que as exceções devem ser consideradas, mas não tratadas como regras que mudem a essência do objeto, do serviço.

Cabe observar que vários critérios e conceitos de riscos, entre os quais jurídicos, técnicos, operacionais, recursos humanos, de negócio dentre muitos outros apresentados na Tabela 4-2, podem ser sopesados pelo gestor, caso ele tenha essa lista prévia para apoiá-lo ao considerar as opções durante o planejamento da contratação.

Adicionalmente, é importante observar que a IN04 atual, implicitamente considera que a Identificação de Riscos siga uma orientação de referência, tanto quantitativamente quanto qualitativamente. Assim, o artefato aqui proposto responde àquela necessidade implícita e, em particular, no aspecto quantitativo, define vários elementos mensuráveis que podem ser considerados e que não existiam formalmente. No que se refere a aspectos qualitativos, como se observa o estado da arte no modelo proposto, pode-se definir que nele estão compiladas contribuições de fontes confiáveis de informação sobre o assunto.

No que se refere à estruturação da pesquisa, os tópicos elencados respondem a hipótese de pesquisa proposta neste trabalho. Ou seja, um artefato baseado no estado da arte de gestão de riscos poderá, sim, otimizar o processo de identificação de riscos da IN04, pois propõe uma abordagem padronizada na maneira de se identificar riscos.

Além disso, a coleção dos elementos apontados pela literatura consultada, comparada à realidade do modelo de Análise de Riscos atual (que em particular tem como ponto de partida um artefato em branco) sugere que a forma apresentada neste trabalho consiste em uma fonte consolidada de conhecimento quando comparada aos diversos modelos e livros que isoladamente tratam sobre o tema de maneira independente.

Assim, identificar riscos com o artefato aqui proposto poderá convergir os esforços na construção de um termo de referência com melhores indicadores de nível de serviço, fator tão ponderado pelos órgãos de controle. A aderência aos níveis de serviço ideais da solução aumenta as chances de êxito da compra ser realizada com base na necessidade real e considerando os riscos e impactos da contratação. A relação entre riscos identificados e nível de serviço adequado é diretamente proporcional, uma vez que o que não é identificado, analisado e tratado não pode ser gerenciado, medido ou quantificado, impactando diretamente na solução de TI contratada.

Dentre as conclusões deste trabalho, pode-se levar em conta que para um bom planejamento da contratação é importante considerar que sejam feitas várias interações e iterações, além de revisões por diferentes pessoas com diferentes perfis. A utilização de um artefato para Identificação de Riscos permitirá uma maturidade maior a cada iteração, gerando possivelmente uma identificação de riscos cada vez mais aderente ao negócio e aprimorando a capacidade de governança do gestor de TI, pessoa responsável pela contratação.

O artefato proposto no trabalho poderá, inclusive, motivar outras contribuições ao processo. Este trabalho tomou a criação do artefato de Identificação de Riscos como eixo, mas isso não impede que essa iniciativa seja utilizada para outros artefatos.

Durante a fase final desta pesquisa, foi observado que o Tribunal de Contas da União (TCU), lançou o Guia de Boas Práticas em Contratação de Soluções de TI (BRASIL, 2012), com o objetivo de contribuir para que os órgãos e entidades da Administração Pública Federal planejem as contratações de bens e serviços de TI, de forma a utilizá-las para alavancar suas operações e entregar os resultados almejados pela sociedade. O trabalho é direcionado para as equipes de TI dos órgãos federais para auxiliar no planejamento das contratações de TI de maneira consistente e sustentável, evitando problemas já conhecidos.

Isso demonstra que alguns pontos a serem melhorados identificados neste estudo, já se tornaram realidade. O TCU compilou uma base de conhecimento com 78 riscos identificados e as devidas ações a serem tomadas, às quais chamou de ‘controle interno’.

Além disso, o guia do TCU aponta o que a legislação, a jurisprudência e as melhores práticas sinalizam sobre o processo de planejamento das contratações de TI, contribuindo assim ainda mais com as atividades de identificação de riscos, objeto de estudo deste trabalho.

Finalmente, não há como negar o fato de que, caso o artefato proposto seja colocado em prática, ele poderá (e, de fato, deverá) ser modificado e adaptado, por se tratar de um modelo generalista e que pode utilizar diversas fontes de conhecimento. Especificamente, é necessário que o artefato seja adaptado à realidade dos órgãos, bastando para isso que sejam considerados os conceitos desejados, e que não mudem a essência do objeto, do serviço. Reitera-se que este modelo é proposto no sentido de agregar ao processo de contratação de TI da APF uma atividade mais detalhada e não se trata de uma crítica formal ao que já existe, pelo contrário, sugere-se inclusive que seja consultado o Guia de Boas Práticas do TCU.

Por fim, vale observar que o artefato proposto no trabalho pode não ser a solução para todos os problemas de identificação de riscos, mas é suficientemente estruturado para apoiar os gestores na identificação dos riscos adicionais, tendo nascido da compilação de boas práticas no domínio. A partir de sua aplicação, é possível agregar a outras fontes de informação (como a do TCU) mais informações numa base de conhecimento, com a contribuição de várias organizações, para aplicação em contratações futuras, melhorando cada vez mais os conceitos, critérios e parâmetros de identificação de riscos, nas diversas organizações públicas brasileiras.

Uma das possibilidades de aplicação do modelo proposto consiste de sua integração às práticas de *Balance Scorecard* (BSC) destinadas ao serviço público, conforme apresentado por Felix et *al*. (2011), artigo em que os autores exemplificam como o BSC pode ser adequado para gestão estratégica nas organizações públicas. Tal pesquisa trata de critérios que podem ser considerados para o artefato aqui proposto, numa perspectiva de contexto a nível de governança, mas que não foram desdobrados neste trabalho, devido ao amplo escopo do tema.

## 6.1 SUGESTÃO DE TRABALHOS E ATIVIDADES FUTURAS

- Automatizar a maneira de se identificar riscos encontrados em cada contratação, por meio de um *workflow* ou sistema de informação.
- Escrever as lições aprendidas das contratações e compartilhar com outros órgãos da APF, por meio de um sistema de informação.
- Montar uma base de conhecimento de riscos da contratação tipo de ativo, ameaças e vulnerabilidades e por tipo de contratação.
- Reavaliação do processo de planejamento da contratação, inserindo o artefato ou a melhoria dele.
- Propor a criação de uma unidade de gestão de riscos das contratações na SLTI ou em órgão que possa apoiar a SLTI para que ela especifique os critérios a serem auditados, em parceria com o TCU.
- Propor a criação de um papel denominado “Gestor de Riscos”, com atribuições de responsabilidade para gerir essas atividades, pois elas são contínuas e não podem se limitar a serem feitas na etapa de planejamento da contratação. Isso possibilita a identificação de quais ações de melhoria de controle que possuem níveis adequados, inadequados ou em excesso.

# REFERÊNCIAS


ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31010. **Gestão de Riscos - Técnicas de Avaliação de Riscos**, Brasil, 2012.

_____. NBR 13790. **Terminologia - Princípios e Métodos - Harmonização de conceitos e termos.** Brasil, 1997.

_____. NBR ISO 31000. **Gestão de Riscos,** Brasil, 2009a.

_____. NBR ISO GUIA 73. **Gestão de Riscos - Vocabulário**, Brasil, 2009b.

_____. NBR ISO/IEC 38500:2009. **Governança Corporativa de Tecnologia da Informação.** Brasil**,** 2009c.

BARBOSA, Alexandre Fernandes; JUNQUEIRA, Álvaro Ribeiro Botelho; LAIA, Marconi Martins de; FARIA, Fernando Inácio de. Governança de TIC e Contratos no Setor Público. In: **CATI - Congresso Anual de Tecnologia da Informação**, 2006, Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (FGV-EAESP), São Paulo, 2006. Disponível em: <http://www.fgvsp.br/cati/artigos/pdf/T00241.pdf>. Acesso em: Maio. 2012.

BERNSTEIN, P.L. **Against the Gods: The Remarkable Story of Risk**. John Wiley e Sons, New York, NY, 1996, p.383.

BRASIL. **Lei nº. 8.666, de 21 de junho de 1993**. Disponível em http://www.planalto.gov.br /ccivil_03/LEIS/L8666cons.htm. Acesso em Maio de 2012.

_____. **Decreto n°. 2.271, de 07 de Julho de 1997**. Dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/D2271.htm. 09 de Janeiro 2011.

_____. **Decreto-Lei n°. 200, de 25 de fevereiro de 1967**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del0200.htm. Acesso em: 30 dez. 2011.

BRIER T. Luftman, J.; Archieved and Sustaitaninig Bussiness ITAlingnament**. California Manegement review**, 42, n.1 Fall, 1999.

CASTRO, Marcelo S. **Análise do perfil do profissional de tecnologia da informação e comunicação a partir da percepção interna do setor**. Tese de Doutorado, Publicação Junho/2010, departamento de Engenharia Elétrica, Universidade de Brasília, DF, 153 p.

CEPIK, Marco; CANABARRO, Diego Rafael. **Governança de TI: Transformando a Administração Pública no Brasil**. – Porto Alegre: WS Editor, 2010.

CHAVAS, Jean-Paul. **Risk analysis in theory and practice**. Elsevier Academic Press, San Diego, 2004.

CRUZ, Cláudio Silva da. **Governança de TI e conformidade legal no setor público: um quadro referencial normativo para a contratação de serviços de TI**. 2008. 252f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação). Universidade Católica de Brasília, Brasília, 2008. Disponível em: http://www.cscruz.org/publico/CRUZ,2008,DissertacaoFinal.pdf . Acesso em: 13 jan. 2012.

_____. Principais cuidados a serem tomados para melhorar os resultados e diminuir riscos. **Apresentação Fórum TI Controle - 5 anos**. Brasília, 2011a.

CRUZ, Cláudio Silva da; ANDRADE, Edméia Leonor Pereira de; FIGUEIREDO, Rejane Maria da Costa. **Processo de Contratação de Serviços de Tecnologia da Informação para Organizações Públicas**. Ministério da Ciência e Tecnologia - Secretaria de Políticas de Informática. Brasília, 2011.

DE CICCO, Francesco e FANTAZZINI, Mário Luiz. **Os riscos empresariais e a gerência de riscos**. Módulo 1 do curso de Gerência de Riscos. São Paulo, 1985.

DE HAES, S.; VAN GREMBERGEN, W. IT governance structures, processes and relational mechanisms: achieving IT/business alignment in a major Belgian financial group. **Proceedings of the 38th Hawaii International Conference on System Sciences**, Hawaii, 2005.

EMBLEMSVAG, Jan; KJOLSTAD, Lars Endre. **Strategic Risk analysis – a field version. Management Decision**. 2002.

FELIX, Rozelito; DO PRADO, Patrícia; DE SOUSA, Rafael Timóteo de. **Balance Scorecard: adequação para a gestão estratégica nas organizações públicas**. Revista do Serviço Público, 62(1) jan/mar, 2011.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI**: **da estratégia à gestão dos processos e serviços**. São Paulo: Brasport, 2008.

FILGUEIRAS, Fernando. **A tolerância à corrupção no Brasil: uma antinomia entre normas morais e prática social.** Departamento de Ciência Política Universidade Federal de Minas Gerais. Nov. 2009.

GASETA, Edson Roberto. **Governança de TI**. Escola Superior de Redes (RPN). Rio de Janeiro, 2011.

GASPAR, Nélio Lima; **Análise Comparativa do Processo de Compras de Serviços de Tecnologia da Informação da Administração Pública Brasileira.** Dissertação de Mestrado. IBMEC. 2005.

GIMENES, Carlos Júnior. **Uma Proposta de Método de Auditoria Focada em Riscos para Melhoria da Qualidade da Informação nas Empresas**. Dissertação (Mestrado) – Programa de Pós-Graduação em Engenharia de Produção. Instituto de Ciências Exatas da Universidade Paulista (UNIP). São Paulo, 2003.

GUALBERTO, E. S. (2011). InfoSecRM: **Uma ontologia para Gestão de Riscos de Segurança da Informação**. Dissertação de Mestrado em Engenharia Elétrica, Publicação 459/2011, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 154p.

GUARDA, Graziela Ferreira (2011). **Análise de Contratos de Terceirização de TI na Administração Pública Federal sob a ótica da Instrução Normativa n° 04**. Dissertação de Mestrado em Engenharia Elétrica, Publicação 437/2011, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 100p.

HAMILTON, S. **Controling risks**. In: MARCHAND. D. A. (ed.), Competing with information: a managers guide to creating business value with information content. Chichester : John Wiley & Sons, 2000. p. 209-228.

HERNANDES, Carlos Alberto Mamede. **Mapeamento de processos de trabalho relativos à contratação de bens e serviços de Tecnologia da Informação no Tribunal de Contas da União.** 2005.

INSTRUÇÃO NORMATIVA Nº 04**. IN04, de 12 de novembro de 2010**. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. 2010c. Disponível em: http://www.governoeletronico.gov.br. Acesso em: 1 mar. 2011.

IT GOVERNANCE INSTITUTE. **COBIT - Control Objectives for Information and related Technology**. 4.1. ed. Rolling Meadows: ITGI, 2007. Disponível em: <http://www.isaca.org/Knowledge-Center/Cobit/Pages/Downloads. aspx>. Acesso em: 10 jan. 2012.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de Serviços de TI na Prática: uma abordagem com base na ITIL**. 1.ed. São Paulo: Novatec, 2007.

MARSHALL, C. **Medindo e Gerenciando Riscos Operacionais em Instituições Financeiras.** São Paulo, Qualitymark Editora, 2002.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO (MP). **Guia de Compras Públicas Sustentáveis para Administração Pública Federal**. Brasília, 2010.

MOTTA, Alexandre Ribeiro da; **Combate ao desperdício no gasto público: uma reflexão baseada na comparação entre o sistemas de compras privado, público federal norte-americano e brasileiro.** Dissertação de Mestrado. Instituto de Economia. Unicamp. 2010.

NETO, João Souza. Alternativas de Diagnóstico de Maturidade COBIT. **4º Encontro de Governança Aplicada – ISACA BRASILIA CHAPTER**. Brasília, 2011.

NOTA TÉCNICA 01/2008. **Conteúdo mínimo do projeto básico ou termo de referência para contratação de serviços de tecnologia da informação - TI**. Tribunal de Contas da União. Brasília, 2008.

NOTA TÉCNICA 02/2008**. Uso do Pregão para aquisição de bens e serviços de Tecnologia de Informação.** Tribunal de Contas da União. Brasília, 2008.

NOTA TÉCNICA 06/2010**. Aplicabilidade da Gestão de Nível de Serviço como mecanismo de pagamento por resultados em contratações de serviços de TI pela Administração Pública Federal.** Tribunal de Contas da União. Brasília, 2010.

OLIVEIRA, César Augusto Dias de; COSTA, Sthéfane Cecília da Silva; **Guia sobre Responsabilidade Compartilhada: O Lixo Agora é problema de todos**. Projeto cidadão. 2010.

OLIVEIRA, Paulo Antonio Fuck de. **Terceirização como Estratégia**. 52ª ed. São Paulo: Atlas, 1996.

PETERSON, R. **Integration strategies and tactics for information technology governance.** In: VAN GREMBERGEN, W. Strategies for information technology governance, Hershey: Idea group publishing, 2004.

PIRES, José Calixto de Souza e MACEDO, Kátia Barbosa. Cultura Organizacional em Organizações Públicas no Brasil. **RAP-Revista de Administração Pública**, v.40, n.1, p. 81-105, Jan./Fev. 2006.

PROJECT MANAGEMENT INSTITUTE - PMI . **Government Extension to a Guide to the Project Management Body of Knowledge**. Newton Square-USA: Project Management Institute, Inc., 2002.

_____. **Guia PMBOK. Um guia do conjunto de conhecimentos em gerenciamento de projetos.** Português. Brasil. 3. ed. 2004.

REZENDE, Denis Alcides. Alinhamento Estratégico da Tecnologia da Informação ao Planejamento Estratégico: proposta de um modelo de estágios para governança em serviços públicos. **Revista de Administração Pública - RAP**, v. 38, n. 4, p. 519-542, Jul./Ago. 2004.

SANTOS, Rildo. **Tecnologia da Informação é fundamental para prestar serviços ao cidadão.** Disponível em: http://www.governoeletronico.gov.br/noticias-e-eventos/noticias/tecnologia-da-informacao-e-fundamental-para-prestar-servicos-ao-cidadao-diz-especialista. Acesso em 02 fev. 2012.

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO (SLTI - Ministério do Planejamento)**. Guia de Prático para Contratação de Soluções de Tecnologia da Informação.** Brasília, 2011. Disponível em: http://www.governoeletronico.gov.br/sisp-conteudo/nucleo-de-contratacoes-de-ti/modelo-de-contratacoes-normativos-e-documen-tos-de-referencia/guia-de-boas-praticas-em-contratacao-de-solucoes-de-ti. Acesso em 10 de janeiro de 2012.

SILVA, Karina Lima da; OLIVEIRA, Marcelle Colares; MARTINS, Márcia Mendes de; ARAÚJO, Osório Cavalcante. **A Implementação dos Controles Internos e do Comitê de Auditoria Segundo a Lei SOX: o Caso Petrobras**. Revista Contabilidade Vista & Revista. Universidade Federal de Minas Gerais, Belo Horizonte, 2009.

SUOMI, Reima e TÄHKÄPÄÄ, Jarmo. **Governance Structures for IT in the Health Care Industry.** In: VAN GREMBERGEN, Win (ed.). Strategies for Information Technology Governance. Hershey, PA, USA: Idea Group Publishing, 2004.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão 786/2006**. Tribunal de Contas da União. Disponível em : http://contas.tcu.gov.br/portaltextual/MostraDocumento?lnk=(acordao+adj+786/2006+adj+plenario)[idtd][b001]. Acesso em: 10 fev. 2012. TCU.

_____. **Guia de boas práticas em contratação de soluções de tecnologia da informação: riscos e controles para o planejamento da contratação** / Tribunal de Contas da União. – Versão 1.0. – Brasília: TCU, 2012. 527 p.

_____. **Acórdão 1.603/2008.** Tribunal de Contas da União. Disponível em: http://contas.tcu.gov.br/portaltextual/MostraDocumento?lnk=(acordao+adj+1603/2008+adj+plenario)[idtd][b001]. Acesso em: 10 fev. 2012.

_____. **Acórdão 2.308/2010.** Tribunal de Contas da União. Disponível em: http://contas.tcu.gov.br/portaltextual/MostraDocumento?lnk=(acordao+adj+2308/2010+adj+plenario) [idtd][b001]. Acesso em: 10 fev. 2012.

_____. **Guia de boas práticas em contratação de soluções de tecnologia da informação: riscos e controles para o planejamento da contratação** / Tribunal de Contas da União. – Versão 1.0. 527p - Brasília, 2012.

WEBBER, Eduard; KHADEMIAN, Anne. Wicked Problems, Knowledge Challenges, and Collaborative Capacity Builders in Network Settings. **Public Administration Review**. Washington State University. March/April 2008.

WEILL, Peter; ROSS, Jeanne**. IT governance on one page**. Center for Information System Research. CISR WP nº. 349 and Sloan WP nº. 4516-04. Massachusetts Institute of Technology, Cambridge. 2004a.

WEILL, Peter; ROSS, Jeanne. **IT governance: how top performers manage IT decisions rights for superior results.** Watertown: Harvard Business School Press, 2004.

WRIGHT, Catherine. Top three potential risks with outsourcing information systems. **Information Systems Control Journal, v. 5,** 2004. Disponível em: http:// www.isaca.org/Content/ContentGroups/Journal1/20044/jpdf045topThreePotentialRisks.pdf. Acesso em: 31 jul. 2011.