Pós-Graduação em Ciência da Computação

Fabiana Ferreira Cardoso

GRATIC: Uma Metodologia para Gestão de Riscos em Aquisições de TIC no Âmbito dos Institutos Federais de Educação

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/∼posgraduacao

Recife

2019

Fabiana Ferreira Cardoso

GRATIC: Uma Metodologia para Gestão de Riscos em Aquisições de TIC no Âmbito dos Institutos Federais de Educação

Trabalho apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre Profissional em Ciência da Computação.

Área de Concentração: Engenharia de Software e Linguagens de Programação.

Orientadora: Carina Frota Alves

Recife

2019

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

C268g Cardoso, Fabiana Ferreira
GRATIC: uma metodologia para gestão de riscos em aquisições de TIC no âmbito dos institutos federais de educação / Fabiana Ferreira Cardoso. – 2019.
189 f.: il., fig., tab.

Orientadora: Carina Frota Alves
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2019.
Inclui referências e apêndices.

1. Engenharia de software. 2. Ineficiência em gestão de riscos. I. Alves, Carina Frota (orientadora). II. Título.

005.1 CDD (23. ed.) UFPE-CCEN 2020-20

Fabiana Ferreira Cardoso

GRATIC: Uma Metodologia para Gestão de Riscos em Aquisições de TIC no Âmbito dos Institutos Federais de Educação

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para obtenção do título de Mestre Profissional em 13 de dezembro de 2019.

Aprovado em: 13/12/2019.

BANCA EXAMINADORA

_____

Prof. PhD. Alixandre Thiago Ferreira Santana

Computer Science / UAG/UFRPE

_____

Profa. PhD. Carina Frota Alves

Centro de Informática / UFPE

(Orientadora)

_____

Profa. PhD. Jéssyka Flavyanne Ferreira Vilela

Centro de Informática / UFPE

Dedico à minha família, pela paciência e compreensão.

AGRADECIMENTOS

Primeiramente agradeço à minha orientadora por acreditar na minha capacidade de superar os desafios que venho enfrentando no decorrer do último ano, pelo incentivo diante das diversidades da vida, pela motivação nos momentos de tristeza, pela orientação e disponibilidade.

A Joelma França pelo carinho e presteza em atender todas as demandas e dúvidas.

A instituição que trabalho e a Secretaria de Educação Profissional e Tecnológica (SETEC) pelo apoio durante as semanas de aulas e custeio do programa de mestrado profissional.

Aos colegas de trabalho e do mestrado profissional pela amizade, companheirismo e parceria. Em especial ao amigo Fagner Costa, Linaldo Leite e a prima Dunya Moraes que fizeram a revisão do documento.

RESUMO

A sistematização da gestão de riscos no setor público é uma das estratégias adotadas pelas entidades públicas para lidarem com as incertezas, uma vez que estimula a transparência, contribui para o uso eficiente de recursos públicos, controla riscos que possam comprometer a eficiência organizacional, busca a melhoria contínua a partir da visão estratégica e permite a sobrevivência das organizações no cenário das constantes mudanças e transformações digitais. Neste contexto, a ineficiência em gerir riscos no processo de aquisição de Tecnologia da Informação e Comunicação (TIC) na Administração Pública Federal tem sido uma das preocupações dos órgãos de controle nos últimos anos, uma vez que este processo pode afetar o valor da TI para os negócios resultando na perda de grandes oportunidades de mudanças e inovação na prestação de serviços públicos. Neste sentido, objetivou-se com este estudo sugerir uma metodologia para gerenciar riscos em aquisições de TIC de forma eficiente no contexto das instituições públicas brasileiras. Para isso, foi desenvolvida uma investigação utilizando o método de pesquisa *Design Science Research*, a metodologia proposta é chamada GRATIC (Gestão de Riscos em Aquisições de Tecnologia da Informação e Comunicação). A metodologia GRATIC foi elaborada a partir dos resultados de questionários e entrevistas com especialistas e foi validada através de estudo de caso em um Instituto Federal de Educação. O estudo contribui para a melhoria contínua do processo de aquisição maximizando a transparência das atividades de gestão de riscos, assim como também disponibiliza um repositório digital de informações contendo as lições aprendidas sobre gestão de riscos no decorrer da pesquisa.

Palavras-chaves: Engenharia de software. Ineficiência em gestão de riscos.

ABSTRACT

The systematization of risk management in the public sector is one of the strategies adopted by public entities to deal with uncertainties. It encourages transparency, contributes to the efficient use of public resources, controls risks that may compromise organizational efficiency, seeks to continuous improvement from the strategic vision and allows the survival of organizations in the scenario of constant changes and digital transformations. In this context, the inefficiency of risk management in the process of acquiring Information and Communication Technology (ICT) in the Federal Public Administration has been one of the concerns of the controlling bodies in recent years, since this process may affect the value of IT to business resulting in the loss of major opportunities for change and innovation in the provision of public services. In this sense, the objective of this study was to suggest a methodology for managing risks in ICT acquisitions efficiently in the context of brazilian public institutions. For this, an investigation was developed using the Design Science Research method. The proposed methodology is called GRATIC (Risk Management in Information and Communication Technology Acquisitions). The GRATIC methodology was elaborated from the results of questionnaires and interviews with experts and was validated through case study in a Federal Institute of Education. The study contributes to the continuous improvement of the procurement process by maximizing the transparency of risk management activities, as well as providing a digital repository of information containing risk management lessons learned throughout the research.

Keywords: Software engineering. Inefficiency in risk management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CGU	Controladoria Geral da União
CIn	Centro de Informática da Universidade Federal de Pernambuco
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
GRATIC	Gestão de Riscos em Aquisições de Tecnologia da Informação e Comunicação
IBGC	Instituto Brasileiro de Governança Corporativa
IFES	Institutos Federais de Educação
ISACA	*Information System Audit And Control Association*
MPOG	Ministério do Planejamento, Orçamento e Gestão
PDCA	*Plan, Do, Check, Action*
SGD	Secretaria de Governo Digital
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

O capítulo tem o objetivo de apresentar a contextualização da pesquisa, o problema e sua importância, a questão que norteia a dissertação, motivações para realização do estudo e objetivos a serem alcançados. Por fim, detalha como a dissertação está estruturada.

1.1 CONTEXTUALIZAÇÃO

De maneira geral, as aquisições que envolvem TIC na Administração Pública Federal (APF) costumam ser bastante complexas e burocráticas, exigindo conhecimento técnico aprofundado no assunto, além de competências para planejar e gerir adequadamente a contratação, de acordo com a legislação vigente (PIRES, 2016; PARREIRA, 2018). Apesar do aporte legal que subsidia o processo de aquisição de TIC, é comum haver divergência entre o que foi planejado e a efetiva execução do contrato, na maioria das vezes ocasionada pela diferença entre preço licitado e o valor praticado pelo mercado.

As divergências ocorridas no processo de aquisições de TIC são preocupantes, pois algumas condições envolvidas são difíceis de serem quantificadas e gerenciadas, como por exemplo, o equilíbrio entre escopo, prazo, custo, qualidade, gestão de mudanças, forma de aceitação do bem ou serviço, transferência de conhecimentos, riscos, dentre outros aspectos (TCU, 2017; 2018d). Neste sentido, estas condições podem gerar várias incertezas e ocasionar diversos riscos para ambas as partes, contratado e contratante, acarretando sérios conflitos durante a execução contratual, podendo gerar problemas para a instituição.

Embora grande parte das instituições públicas sigam um modelo de gestão de riscos definido na legislação vigente (BRASIL, 2016), a gestão de riscos não é realizada de forma eficiente em todas as fases do processo de aquisição de TIC (TCU, 2018g). A falta de procedimentos sistemáticos faz com que os riscos envolvidos durante a contratação de TIC não sejam efetivamente gerenciados, podendo acarretar insucesso no alcance das metas e objetivos organizacionais (TCU, 2018f).

Para o TCU (2018e) a boa governança em contratações evita ou reduz processos de planejamento inadequados, projetos mal sucedidos e/ou contratações que não alcançam seus objetivos, implicando prejuízos, perdas de qualidade e ineficiências. Órgãos de controle, como o Tribunal de Contas da União (TCU) têm reportado nos últimos anos suas preocupações, uma vez que as incertezas afetam o valor da TI para o negócio (TCU, 2017; 2018d).

No levantamento realizado em 2017, o TCU mostrou que 86% das organizações que preencheram o questionário de avaliação sobre governança pública brasileira, declararam que não estabeleciam diretrizes para gerir riscos nos processos de aquisição e 88% não realizavam nenhuma gestão de riscos em cada contratação específica (TCU, 2017). No relatório de acompanhamento divulgado em 2018 este órgão de controle mostrou que das 498 organizações públicas federais que preencheram o levantamento de governança pública, 71% ainda não reconhecem a importância da gestão de riscos para o processo de contratação de TIC (TCU, 2018f).

De acordo com o sumário executivo IGC 2018 (TCU, 2018e), poucas organizações praticam a análise de riscos das contratações relevantes. Segundo o TCU (2017) o desconhecimento acerca dos riscos relacionados às contratações pode trazer consequências adversas para a organização. Dentre elas tem-se o insucesso no alcance das metas da área de gestão de contratações e a perda de investimento por contratações que não atendem às necessidades da organização.

Dentro do panorama apresentado, há muito o que melhorar uma vez que a maioria das instituições públicas continuam no estágio inexpressivo e inicial de gestão de riscos (TCU, 2018e). Observando sob esta perspectiva, a baixa maturidade em gestão de riscos em aquisições de TIC ocasionada pela falta de procedimentos padronizados para monitoramento e controle de riscos, pode resultar na perda de grandes oportunidades de mudanças e inovação na prestação de serviços públicos. Para o TCU (2018e) a ausência de elementos que permitam o gestor avaliar e mitigar os riscos de TIC em determinado projeto pode desencorajá-lo a executar iniciativas com potencial realmente transformador para a sociedade.

1.2 PROBLEMA

No Brasil, são poucos os órgãos e entidades públicas que possuem políticas ou práticas de gestão de riscos formalmente estabelecidas (TCU, 2018d; 2018e; 2018f; 2018g). A gestão de riscos vêm se tornando ao longo dos anos, um grande desafio enfrentado pelas instituições públicas e tem preocupado os órgãos de controle como o TCU, uma vez que as entidades da APF vêm demonstrando durante as auditorias sobre governança pública, pouca capacidade de governança e gestão de riscos em suas contratações (TCU, 2018e).

De acordo com os dados divulgados pelo TCU (2018e), uma grande parcela das instituições que compõem a APF não gerencia efetivamente seus riscos no processo de aquisições de TIC. Este fato tem acarretado na maioria das vezes excesso de questionamentos, impugnações e recursos por parte das empresas licitantes. Quando os procedimentos licitatórios não são gerenciados de forma sistematizada e eficiente, comprometem a execução das atividades fins das instituições, consequentemente a qualidade na prestação de serviços públicos.

A partir das informações apresentadas pelo TCU (2018e), pode-se afirmar que a ineficiência em gerir riscos em aquisições de TIC, problema a ser estudado nesta pesquisa, está relacionada à falta de procedimentos práticos, padronizados e sistematizados para identificar, avaliar, tratar, monitorar, controlar, comunicar riscos que ocorrem durante a execução das fases do processo de aquisição de TIC. Embora existam normativas sobre gestão de riscos em aquisições de TIC, as instituições têm dificuldades em administrar riscos relacionados a contratações de TIC (TCU, 2018f; 2018g).

Neste sentido, observa-se que este problema é recorrente na APF e traz uma série de consequências que podem ocasionar sérios transtornos e prejuízos para as instituições públicas. O fracasso ou atraso no processo de aquisição de TIC, motivado pela ineficiência na gestão de riscos, pode acarretar atrasos na atualização do parque tecnológico, o que impacta diretamente na execução de projetos sociais, políticos, econômicos, educacionais entre outros.

A falta de conhecimento para realizar a análise de riscos compromete o bom funcionamento do processo aquisitivo, podendo causar atrasos consideráveis na

entrega de recursos tecnológicos, necessários para o cumprimento da missão institucional. A inexistência de suporte e garantia de equipamentos, pode indisponibilizar sistemas informatizados essenciais para a sociedade. A interrupção da prestação de serviços continuados como link de internet, datacenter ou locação de equipamentos, inviabiliza o trabalho dos servidores públicos.

Diante do panorama apresentado, o TCU (2018f) em seu relatório técnico completo de acompanhamento de governança pública, relata que a incipiência na gestão de riscos na área de TIC é grave, haja vista a criticidade dos serviços de tecnologia da informação para algumas organizações. Neste sentido, a ocorrência de algum evento adverso na área de TI na esfera pública, pode resultar na suspensão total da prestação de serviços públicos essenciais para a sociedade.

Com o intuito de compreender o fenômeno apresentado e propor uma solução para o problema identificado no capítulo 4, objetiva-se com essa pesquisa investigar: ***"como realizar de forma eficiente a gestão de riscos em aquisições de TIC nas instituições públicas brasileiras?"***.

Na busca de uma possível solução para o problema relatado no capítulo 4, o contexto dos Institutos Federais de Educação foi escolhido por conveniência, pela facilidade de acesso às informações, proporcionando assim uma amostra maior, aumentando a confiabilidade dos dados obtidos. Como os riscos relacionados ao processo de aquisição de TIC são semelhantes em todas as entidades públicas que fazem parte da Administração Pública Federal, a solução a ser proposta neste estudo poderá ser utilizada por outras instituições públicas brasileiras.

1.3 MOTIVAÇÕES

O TCU tem realizado periodicamente o levantamento de informações relativas a governança pública buscando identificar vulnerabilidades e contribuir com a melhoria da administração pública brasileira. Para este órgão de controle o cenário é preocupante, uma vez que é o mesmo desde 2014 em relação à gestão de riscos e não há sinalização de que exista tendência para melhora verificável (TCU, 2018e).

Grande parte das Instituições Federais de Educação estão no estágio inexpressivo ou inicial de capacidade de gestão de riscos em aquisições de TIC

(TCU, 2018g). Com base na avaliação dos dados apresentados no relatório individual de respondentes (arquivos individuais de cada instituição), referente ao questionário de auto avaliação de governança pública divulgado pelo TCU em 2018, observa-se que em relação as 65 universidades que responderam o levantamento (ciclo 2018), apenas 9 estão no estágio aprimorado em gerir riscos, 3 estão no estágio intermediário e as demais no estágio inicial ou inexpressivo (TCU, 2018g).

Em relação aos 44 institutos presentes no relatório, apenas 6 estão no estágio aprimorado e 2 no intermediário de capacidade em gestão de riscos em aquisições de TIC, os demais estão no nível inexpressivo ou inicial (TCU, 2018g). Estes dados demonstram que muito ainda tem que ser feito para tornar a gestão de riscos eficiente no processo de aquisição de TIC.

No âmbito dos institutos que pertencem a rede de educação tecnológica percebe-se através dos relatos apresentados no capítulo 4 que a situação é crítica. Em relação aos 18 institutos federais de educação que participaram desta pesquisa (capítulo 4), 66,7% das instituições afirmam que a gestão de riscos no processo de aquisições de TIC é ineficiente. Neste sentido, medidas devem ser tomadas pela alta gestão com a finalidade de enfrentar os riscos e fornecer condições razoáveis para que a missão e os objetivos organizacionais sejam alcançados.

Em razão da complexidade da temática, a rotatividade dos atores envolvidos no processo de aquisição de TIC e as particularidades de cada equipe de planejamento da contratação, faz se necessário definir procedimentos práticos e sistematizados a serem adotados para identificar, analisar, avaliar, tratar, monitorar, controlar, documentar e informar riscos envolvendo o processo de aquisição de TIC. Além disso, é importante ter o registro das atividades referentes à gestão de riscos durante a execução do processo aquisitivo, de forma que possa agilizar o aprendizado e dar transparência para os atos administrativos conforme recomenda a legislação vigente.

Outro incentivo para o estudo foi a percepção de que na literatura científica, até então construída, sobre gestão de riscos em aquisições de TIC nas entidades que compõem a APF, aborda apenas a Instrução Normativa SLTI Nº 4/2014 que foi revogada em 2019. Atualmente a legislação que rege o processo de contratação de soluções de TIC é a Instrução Normativa SGD/ME Nº 1/2019 (BRASIL, 2019b).

A partir de pesquisas realizadas nos sites dos institutos federais de educação e site compras governamentais, pode-se afirmar que cada instituição realiza a gestão de riscos no processo de aquisição de TIC de forma diferente. Esta pesquisa trata um tema importante, pois foca o aprendizado organizacional, a padronização de procedimentos e rotinas de trabalho e a transparência da gestão de riscos em aquisições de TIC.

Além de ser uma pesquisa que estuda o contexto atual das instituições públicas no Brasil, está em conformidade com a Instrução Normativa SGD/ME Nº 1/2019 de 4 de abril de 2019 (BRASIL, 2019b), Instrução Normativa MPOG Nº 5/2017 de 25 de setembro de 2017 e Instrução Normativa Conjunta MP/CGU Nº 1/2016 de 10 de maio de 2016.

Embora existam várias metodologias de gestão de riscos (MPOG, 2017; NOBRE, 2017; CGU, 2018, TCU, 2018), não foi possível identificar uma abordagem prática, padronizada, sistemática e transparente envolvendo o aprendizado sobre gestão de riscos em todas as fases de aquisição de TIC (planejamento da contratação, seleção do fornecedor e gestão do contrato). Apesar do capítulo 2 apresentar algumas metodologias desenvolvidas pelos órgãos públicos e privados com suas características, estrutura e processo de gestão de riscos, elas não abordam de forma transparente os procedimentos práticos a serem adotados em cada fase do processo de aquisição de TIC.

Não foi encontrado nas metodologias de gestão de riscos apresentadas na tabela 1, um catálogo contendo riscos e controles sistematizados para auxílio das atividades de identificação, avaliação e tratamento de riscos. Uma planilha documentadora contendo diversos riscos e controles mapeados por outros especialistas na área de aquisições de TIC, é uma das contribuições desta pesquisa para a melhoria do processo.

A tabela 1 apresenta o quadro comparativo entre a solução apresentada neste estudo as metodologias apresentadas no capítulo 2. A comparação envolve as atividades: Identificação de Riscos (IR), Avaliação de Riscos (AR), Tratamento de Riscos (TR), Monitoramento de Riscos (MR), Controle de Riscos (CR), Documentação de Riscos (DR), Comunicação e Informação sobre Riscos (CIR), Aprendizado sobre Riscos (APR) e Transparência (TRA).

Tabela 1 - Comparativo entre Metodologias de Gestão de Riscos

Metodologia	IR	AR	TR	MR	CR	DR	CIR	APR	TRA	Referência
MGR-INSS (CASTRO, 2014)		X								IN04/SLTI RMM/CMMI-ACQ/COBIT
MGR-SISP (MPOG, 2016)	X	X	X	X			X			INC CGU/MP 1/2016 ISO 27005 IN04/SLTI
MGR-GIRC (MPOG, 2017b)	X	X	X				X			COSO ERM
MGR-CGU (CGU, 2018)	X	X	X	X			X			COSO/ISO 31000/IN CGU/MP Nº 01/2016
MGR-Funasa (NOBRE, 2017)	X	X	X	X	X		X			ISO 31000/31010
MGR-IBGC (IBGC, 2017)	X	X	X	X	X					*The Orange Book*
MGR-TCU (TCU, 2018)	X	X	X	X	X		X			*COSO/ ISO 31000 The Orange Book*
MGR-ForRisco (BERMEJO, 2019)	X	X	X	X	X	X	X			COSO/ISO 31000/ THE ORANGE BOOK/ MGR-SISP
MGR-IBGE (IBGE, 2019)	X	X	X	X	X	X				ISO 31000
MGR-GRATIC (CARDOSO, 2019)	X	X	X	X	X	X	X	X	X	ISO 31000/ THE ORANGE BOOK / COSO

Conforme apresenta a tabela 1, o diferencial deste estudo em relação às demais abordagens de gestão de riscos está no fato de que a solução a ser proposta nesta dissertação possibilita a transparência, o aprendizado e compartilhamento de lições aprendidas envolvendo gestão de riscos em aquisições de TIC no decorrer de todas as fases do processo licitatório através de uma planilha documentadora disponibilizada em um repositório digital de informações.

A partir da definição do problema e motivações para realização desta pesquisa, o objetivo geral e os específicos foram detalhados. A próxima seção irá realizar o detalhamento dos objetivos.

1.4 OBJETIVOS

Este estudo tem como objetivo geral ***propor uma metodologia para gerenciar riscos em aquisições de TIC de forma eficiente no contexto das Instituições Públicas Brasileiras.*** Para que os resultados esperados sejam alcançados foram definidos os seguintes objetivos específicos:

- Pesquisar abordagens práticas sobre gestão de riscos utilizadas pelas instituições públicas brasileiras.
- Identificar técnicas, ferramentas, artefatos e procedimentos já usados no contexto público, de forma a sistematizar atividades para a gestão de riscos em aquisições de TIC.
- Aplicar questionários e entrevistas com algumas entidades públicas que fazem parte do poder executivo federal com intuito de conhecer e compreender os principais problemas, causas e dificuldades relacionadas à gestão de riscos em aquisições de TIC.
- Definir a sequência de procedimentos a serem realizados para identificar, analisar, avaliar, tratar, monitorar, controlar, documentar e relatar riscos em todas as fases do processo de aquisições de TIC.

1.5 ESTRUTURA DA DISSERTAÇÃO

Para que os objetivos estabelecidos sejam alcançados a dissertação está estruturada em 7 (sete) capítulos:

- **Capítulo 1 -** Introdução: apresenta a contextualização da pesquisa, o problema e questão da pesquisa, motivações, objetivos a serem alcançados e a estrutura da dissertação.

- **Capítulo 2 -** Referencial Teórico: descreve o estado da arte em relação à temática da pesquisa. Apresenta a revisão bibliográfica abordando aquisições de TIC, conceitos envolvendo riscos, abordagens e metodologias de gestão de riscos utilizadas por algumas instituições públicas brasileiras que influenciaram o estudo. Finaliza com a análise crítica sobre gestão de riscos.

- **Capítulo 3 -** Metodologia: descreve o método de pesquisa *Design Science Research* abordando as etapas, as estratégias, procedimentos e técnicas utilizados na condução desta pesquisa. Apresenta o método de investigação, métodos e técnicas de coleta de dados, método de análise e síntese de dados e como foi realizada a revisão bibliográfica.

- **Capítulo 4 -** Investigação do Problema: aborda a *investigação do problema* de pesquisa e sua importância a partir da avaliação da situação atual das instituições públicas, o estado atual da gestão de riscos em aquisições de TIC nos institutos federais de educação, as causas para a dificuldade em gerir riscos e os requisitos necessários para desenvolvimento de uma solução para a gestão de riscos em aquisições de TIC.

- **Capítulo 5 -** Design da Solução: descreve a solução desenvolvida detalhando a metodologia GRATIC, seu processo de gestão de riscos, técnicas, ferramentas, artefatos e procedimentos.

- **Capítulo 6 -** Demonstração e Avaliação: detalha o estudo de caso realizado para avaliar e validar a solução proposta nesta dissertação e os sujeitos de pesquisa. Em seguida, avalia o uso da solução, apresenta os resultados obtidos e a avaliação feita pelos participantes do estudo de caso. Em seguida, mostra as contribuições dos especialistas na área de licitações. Por fim, faz uma análise crítica.

- **Capítulo 7 -** Conclusões, Limitações e Trabalhos Futuros. Expõe as considerações finais, trabalhos relacionados à temática da pesquisa, as limitações da pesquisa, principais contribuições e perspectivas futuras.

2 REFERENCIAL TEÓRICO

O capítulo apresenta a revisão bibliográfica necessária para o melhor entendimento da pesquisa. Inicialmente, explora os conceitos envolvendo aquisições de Tecnologia da Informação e Comunicação no setor público. Em seguida, detalha as abordagens sobre gestão de riscos apresentando algumas metodologias que influenciaram este estudo. E por fim, faz uma análise crítica sobre gestão de riscos.

2.1 AQUISIÇÕES DE TIC

Aquisições de TIC no setor público refere-se ao processo de contratação de equipamentos, bens e serviços relacionados à área de TIC, utilizados de forma a prestar serviços de qualidade para a sociedade. No âmbito do Poder Executivo Federal este processo é disciplinado pela Instrução Normativa SGD/ME Nº 1/2019 (BRASIL, 2019b).

A legislação vigente exige que as contratações devem estar alinhadas com o PDTIC do órgão ou entidade, com o plano anual de contratações (PAC) e com a política de governança digital (Decreto Nº 8.638/2016). Se a contratação tiver por objetivo a oferta digital de serviços públicos deve estar integrado à Plataforma de Cidadania Digital (Decreto Nº 8.936/2016) (BRASIL, 2019b).

Além de simplificar os procedimentos, as instruções normativas Nº 1/2019 e 2/2019 asseguram que a APF priorizará a melhoria dos serviços ao cidadão, aprimorando os investimentos no setor de TIC. A Instrução Normativa SGD/ME Nº 1/2019 amplia a responsabilidade dos gestores públicos no processo de contratação e privilegia o planejamento, com ênfase na análise comparativa das soluções e nas justificativas das escolhas. A partir desta publicação passa a ser obrigatória a transparência dos estudos técnicos preliminares na internet, mesmo quando se tratar de contrato com empresas públicas (BRASIL, 2019b).

Possivelmente este fato tenha ocorrido em razão do processo ser complexo e burocrático (PARREIRA, 2018). Os procedimentos licitatórios se fundamentam no cumprimento de prazos e disposições legais amparados pela Constituição Federal

e legislações pertinentes para aquisições que nem sempre são compreendidos pelos envolvidos. No rol das várias leis que regem as contratações, destacam-se:

- Lei Nº 8.666/93, de 21 de junho de 1993.
- Lei Nº 10.520/2002, de 17 de julho de 2002.
- Decreto nº 10.024, de 20 de setembro de 2019.
- Instrução Normativa MPOG Nº 5/2017, de 25 de maio de 2017.
- Instrução Normativa SEGES/ME Nº 1/2019, de 10 de janeiro de 2019.
- Instrução Normativa SGD/ME Nº 1/2019, de 4 de abril de 2019.
- Instrução Normativa SGD/ME Nº 2/2019, de 20 de setembro de 2019.
- Portaria SGD/ME Nº 778/2019, de 4 de abril de 2019.
- Decreto Nº 9.507/2018, de 21 de setembro de 2018.
- Decreto nº 3.555/2000, de 8 de agosto de 2000.
- Decreto Nº 5.450/2005, de 31 de maio de 2005.
- Decreto Nº 7.174/2010, de 12 de maio de 2010.
- Decreto Nº 7.892/2013, de 23 de janeiro de 2013.
- Decreto Nº 8.638/2016, de 15 de janeiro de 2016.
- Decreto Nº 8.936/2016, de 19 de dezembro de 2016.
- Acórdão TCU 4330/2014, de 12 de agosto de 2014.
- Acórdão TCU 2110/2015, de 26 de agosto de 2015.

Estas normativas definem como deve ser o planejamento anual de contratação nas instituições públicas; como é estabelecido o processo de contratação de soluções de TI na APF; as regras e diretrizes do procedimento de contratação de serviços; procedimentos para realização do pregão eletrônico nas aquisições de bens e contratações de serviços comuns; obrigatoriedade da realização da gestão de riscos nas aquisições de TIC; e governança de TIC nos órgãos e entidades pertencentes ao sistema de Administração de Recursos de TI do poder Executivo Federal - SISP.

A quantidade de normativas existentes atualmente tem exigido da equipe de planejamento uma constante capacitação em razão das mudanças nas regras do processo licitatório. Devido a atualização de leis, decretos e normativas sobre aquisições, cada dia que passa o processo de aquisições de TIC tem se tornado difícil e exposto a sérios problemas. A partir de pesquisas realizadas no site

compras governamentais observa-se que grande parte dos problemas que ocorrem durante o processo de aquisição, estão relacionados a erros e omissões na construção do termo de referência e edital de licitação (BRASIL, 2019d).

Em virtude das mudanças que ocorrem ao longo da execução do processo licitatório, percebe-se que os prazos para a aquisição nem sempre são cumpridos em razão do excesso de questionamentos, impugnações e atrasos no cumprimento do contrato. Esta situação tem acarretado em alguns casos o não atendimento das necessidades do negócio (TCU, 2017; 2018d). Dentro deste cenário, vários eventos surgem ocasionando incertezas que podem impactar diretamente na execução da missão e objetivos finalísticos das instituições públicas.

Segundo Parreira (2018) as contratações de soluções de TI por órgãos públicos brasileiros visam atender as necessidades de negócio da organização contratante, buscando o alinhamento entre a sua estratégia e a legislação brasileira. Os princípios de eficiência, eficácia, efetividade, economicidade, legalidade, impessoalidade e publicidade norteiam o contexto acerca das contratações (CRUZ, 2011).

No setor público brasileiro, a contratação de TI tem sido alvo de duras críticas (PARREIRA, 2018). Alguns autores têm reportado problemas e citam fatores que podem prejudicar o processo de contratação, como a falta de alinhamento do planejamento de contratação com o planejamento estratégico da instituição, a falta de formalização do processo, a falta de treinamento e capacitação da equipe e as deficiências durante o processo de gestão e execução do contrato (CRUZ, 2008; GUARDA, 2011; SOARES NETTO, 2013; SILVA, 2016).

Pires (2016), Nobre (2017) e Souza (2017) afirmam que as dificuldades relacionadas ao processo de aquisição de TIC geram incertezas envolvendo recursos financeiros, humanos, materiais e tecnológicos, o que traz diversos riscos e insegurança para os gestores. Sabe-se que as incertezas, na maioria das vezes, ocasionam interrupção do processo licitatório, atrasos na entrega de bens e serviços e até mesmo fracasso no processo de aquisição.

2.1.1 Processo de Aquisição de TIC

O macroprocesso de aquisição de TIC adotado no âmbito das instituições públicas brasileiras é composto por três fases: planejamento da contratação, seleção do fornecedor e gestão do contrato. A figura 1 apresenta o processo contemplando todas as fases obrigatórias para contratação de soluções de TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.

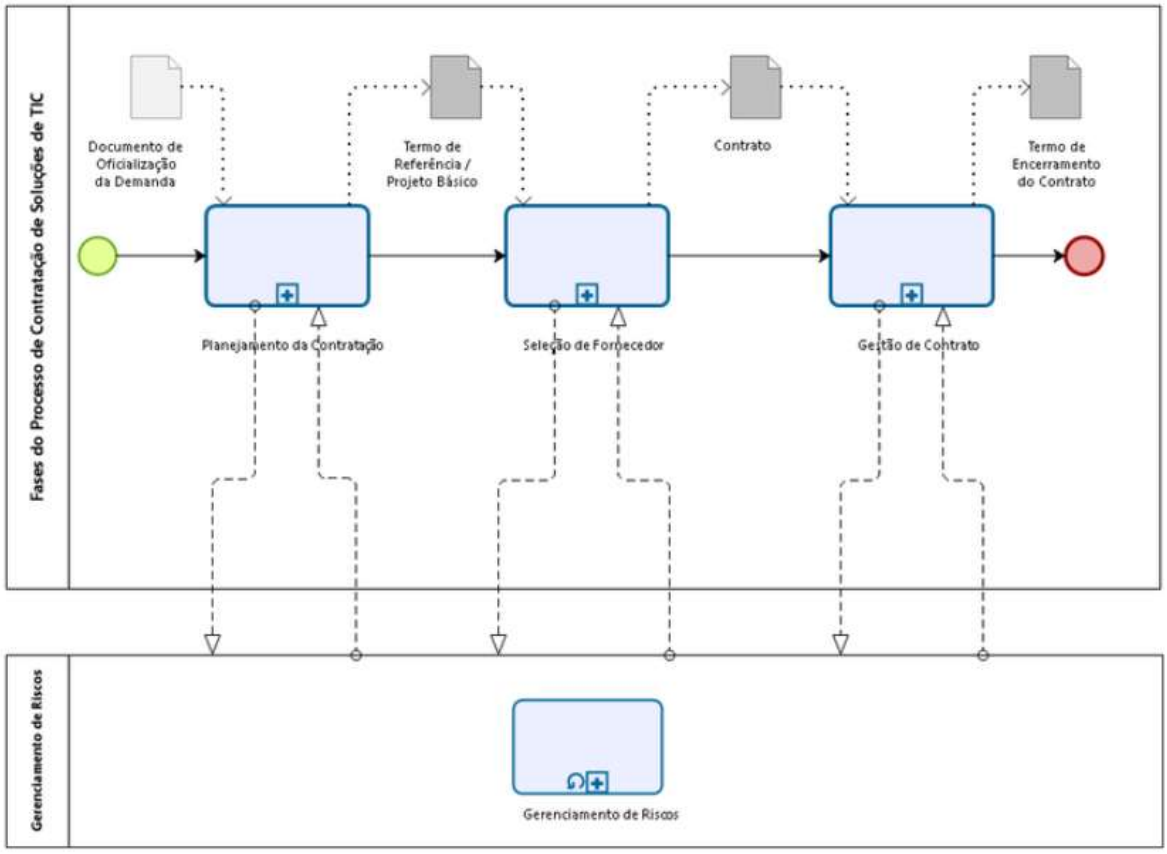


Figura 1 – Modelo de Contratação de Soluções de TIC

O modelo demonstrado na figura 1 apresenta as três fases do macroprocesso de contratações de soluções de TIC proposto pelo governo federal, são elas: planejamento da contratação, seleção do fornecedor e gestão do contrato. Artefatos são utilizados como subsídio para o controle de riscos, como por exemplo: documentos de oficialização de demanda, termo de referência/projeto básico, contrato e termo de encerramento do contrato. Além disso, traz o Gerenciamento de Riscos sendo feito em todas as fases do processo aquisitivo.

O modelo de contratação de soluções de TIC (BRASIL, 2019b) divulgado pela Secretaria do Governo Digital do Ministério da Economia detalha as seguintes fases:

a) **Planejamento da Contratação:** consiste nas etapas de instituição da equipe de planejamento da contratação, elaboração do estudo técnico preliminar da contratação e elaboração do termo de referência ou projeto básico. Independentemente do tipo de contratação as etapas devem ser realizadas obrigatoriamente. Durante a fase de planejamento, a equipe de Planejamento da Contratação deve proceder às ações de gerenciamento de riscos e produzir o Mapa de Gerenciamento de Riscos.
b) **Seleção do Fornecedor:** deve observar as normas pertinentes, incluindo o disposto na Lei Nº 8.666, de 1993, na Lei Nº 10.520, de 2002, no Decreto Nº 9.507, de 2018, no Decreto nº 3.555, de 2000, no Decreto Nº 5.450, de 2005, no Decreto Nº 7.174, de 2010, e no Decreto Nº 7.892, de 2013, e respectivas atualizações supervenientes. Esta fase inicia com o encaminhamento do Termo de Referência ou Projeto Básico pela Área de TIC à Área de Licitações e encerra-se com a publicação do resultado da licitação após a adjudicação e a homologação. Caberá à Área de Licitações conduzir as etapas da fase de Seleção do Fornecedor, e à Equipe de Planejamento da Contratação, durante a fase de Seleção do Fornecedor, analisar as sugestões feitas pelas Áreas de Licitações e Jurídica para o Termo de Referência ou Projeto Básico e demais documentos de sua responsabilidade, apoiar tecnicamente o pregoeiro ou a Comissão de Licitação na resposta aos questionamentos ou às impugnações dos licitantes e apoiar tecnicamente o pregoeiro ou a Comissão de Licitação na análise e julgamento das propostas e dos recursos apresentados pelos licitantes e na condução de eventual Prova de Conceito. Durante a fase de Seleção do Fornecedor, o Integrante Administrativo com apoio dos Integrantes Técnico e Requisitante deve proceder às ações de gerenciamento dos riscos e atualizar o Mapa de Gerenciamento de Riscos.
c) **Gestão do Contrato:** inicia com a assinatura do contrato e com a nomeação dos seguintes integrantes da Equipe de Fiscalização do

> Contrato: Gestor do Contrato, Fiscal Técnico do Contrato, Fiscal Requisitante do Contrato e Fiscal Administrativo do Contrato. A fase de Gestão do Contrato visa acompanhar e garantir a adequada prestação dos serviços e o fornecimento dos bens que compõem a solução de TIC durante todo o período de execução do contrato. Durante esta fase a Equipe de Fiscalização do Contrato, sob coordenação do Gestor do Contrato, deverá proceder atualização contínua do Mapa de Gerenciamento de Riscos.

O Mapa de Gerenciamento de Riscos proposto pela Secretaria do Governo Digital do Ministério da Economia deve ser assinado pela Equipe de Planejamento da Contratação, nas fases de Planejamento da Contratação e de Seleção de Fornecedores, e pela Equipe de Fiscalização do Contrato, na fase de Gestão do Contrato.

2.2 GESTÃO DE RISCOS

A sistematização da gestão de riscos em nível institucional constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, estimula a transparência, contribui para o uso eficiente de recursos públicos e melhora a entrega de serviços ao cidadão (TCU, 2018b). O gerenciamento de riscos é importante para qualquer instituição, uma vez que controla riscos que possam comprometer a eficiência organizacional, busca melhoria contínua a partir da visão estratégica e permite a sobrevivência das organizações no cenário das constantes mudanças e transformações digitais.

Souza (2017) afirma que o processo de gestão de riscos envolve: análise do contexto de determinado processo ou atividade, identificação do que pode dar errado no processo, avaliação do tamanho do potencial problema, definição da forma de tratamento para evitar que a situação aconteça e monitoramento para verificar se o que foi implantado está funcionando ou se há necessidade de ajustes. Nesta perspectiva, ao identificar, analisar, avaliar e desenvolver estratégias de contingenciamento de riscos, deve-se incentivar a proatividade e não na reatividade, tornando o controle de riscos estruturado e eficiente.

Neste sentido, a gestão do risco na área de TI envolve processos, políticas e estruturas que proporcionam conhecer o nível empresarial do risco de TI na empresa. O controle do risco estruturado, administrado adequadamente pelas corporações, ocasiona a redução de custos ou problemas operacionais relacionados as ameaças inerentes ao ambiente da TI, uma vez que visa a redução destes impactos (WESTERMAN; HUNTER, 2008).

Dentro desta perspectiva, quando a gestão de riscos é implementada de forma adequada, traz uma série de benefícios. Dentre eles, Hopkin (2018) cita o fornecimento de informações estruturadas adicionais para auxiliar a tomada de decisão, a melhoria da eficiência das operações, a garantia de que os processos de negócios sejam eficazes e que a estratégia forneça exatamente o que é necessário à entrega eficaz de projetos e programas de trabalho.

Portanto, para que as instituições públicas possam realizar a gestão de riscos na área de TI de forma proativa é essencial que compreenda os conceitos e abordagens envolvidas. Em pesquisas realizadas através de revisão bibliográfica foram identificadas diversas definições sobre riscos e gestão de riscos. As próximas seções irão apresentá-las.

2.2.1 Definições

Geralmente risco é considerado pela maioria dos *frameworks* de gestão de riscos como sendo evento, acontecimento ou situação que é avaliado em termos de consequência, probabilidade e impacto. A fim de que um risco se materialize, um evento deve ocorrer.

Para evitar problemas relacionados a riscos, COSO (2004) recomenda executar a gestão de riscos envolvendo todos os processos de negócios. Isso contribui para assegurar comunicação eficaz e o cumprimento de leis e regulamentos, bem como evita danos à reputação da organização (MPOG, 2017b). Nesta linha de raciocínio, a tabela 2 apresenta as definições de risco, publicadas por algumas organizações no Brasil e no mundo.

Tabela 2 - Definição de Risco

Organização	Definição de risco
COSO (COSO, 2004; 2007; 2017)	Possibilidade de um evento ocorrer e afetar o alcance dos objetivos.
Ferma (FERMA, 2003)	Combinação da probabilidade de um acontecimento e das suas consequências. O simples fato de existir atividade, abre a possibilidade de ocorrência de eventos ou situações cujas as consequências constituem oportunidades para obter vantagens (lado positivo) ou então ameaças ao sucesso (lado negativo).
Institute of Internal Auditors (IIA, 2009)	A incerteza de um evento ocorrendo que poderia ter um impacto no alcance dos objetivos. O risco é medido em termos de consequências e probabilidade.
Institute of Risk Management (IRM, 2002)	Combinação da probabilidade de um evento e sua consequência. As consequências podem variar de positivas a negativas.
ISO Guide 73 (ISO, 2005)	Efeito da incerteza nos objetivos. Um efeito pode ser positivo, negativo ou um desvio do esperado. Um risco é descrito por um evento, uma mudança nas circunstâncias ou uma consequência.
ISO 31000 (ISO, 2009; 2018)	Efeito da incerteza nos objetivos. É um desvio em relação ao esperado. Pode ser negativo, positivo ou ambos e pode abordar, criar ou resultar em oportunidades e ameaças.
M_o_R-OGC (OGC, 2010)	Um evento ou conjunto de eventos incertos que, caso ocorram, terão um efeito no alcance dos objetivos.
Orange Book (OGC, 2004; HMG, 2019)	Incerteza do resultado, dentro de um intervalo de exposição, resultante de uma combinação do impacto e da probabilidade de eventos potenciais. Um evento incerto ou conjunto de eventos que, se ocorrer, terá um efeito sobre a realização dos objetivos. Um risco é composto por uma combinação da probabilidade de uma ameaça ou uma oportunidade de ocorrência e a magnitude do seu impacto sobre os objetivos.
CGU (CGU, 2018)	Possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização.
PMI (2013, 2017)	Evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo em um ou mais objetivos do projeto, tais como: escopo, cronograma, custo e qualidade. Um risco pode ter uma ou mais causas e, se ocorrer, pode ter um ou mais impactos. Uma causa pode ser um requisito, premissa, restrição ou condição potencial que crie a possibilidade de resultados negativos ou positivos.
TCU (TCU, 2018c)	Possibilidade de que um evento afete negativamente o alcance dos objetivos.

As definições de riscos apresentadas na tabela 2 são similares, com algumas peculiaridades envolvendo probabilidade ou possibilidade de ocorrência de determinado evento e impacto dentro da organização. Com base nos conceitos

apresentados é possível observar que riscos estão relacionados à incerteza da ocorrência de eventos ou situações que possam impactar positivamente ou negativamente na missão e/ou nos objetivos organizacionais. A partir dos conceitos observa-se que estão relacionados a vários fatores: pessoa, processo, sistema, tecnologia, infraestrutura e evento externo (ENAP, 2019).

De acordo com o guia PMBOK (PMI, 2017), toda organização deve ter listas de categorias de risco. A classificação dos diversos tipos de riscos é um componente essencial para um programa de gestão de riscos eficiente.

Categorizar as ameaças e oportunidades ajuda a alta gestão a evitar surpresas, ter uma abordagem estruturada e focada para identificar problemas. Além disso, auxilia no desenvolvimento de técnicas eficientes para mitigação de riscos, construir estratégias mais eficazes para responder aos riscos e melhorar o monitoramento de riscos. A Instrução Normativa Conjunta MP/CGU Nº 1/2016 define que os órgãos e entidades do Poder Executivo Federal, ao efetuarem o mapeamento e avaliação dos riscos, deverão considerar, entre outras possíveis, as seguintes tipologias de riscos:

a) riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

b) riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.

c) riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.

d) riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Neste sentido, a maioria dos conceitos sobre gestão de riscos possuem definições convergentes, relacionando riscos com a ocorrência de eventos e seus resultados sobre os objetivos organizacionais (FRANCO, 2017). Sendo assim, para realizar a gestão de riscos de forma adequada é importante compreender as diversas abordagens e estratégias adotadas pelos modelos de referência de forma a identificar qual se adapta a realidade da organização.

Dentro deste raciocínio, a tabela 3 mostra algumas abordagens sobre a temática. Observa-se a partir das definições apresentadas, que gestão de riscos é o processo de planejamento, organização e controle de recursos humanos e materiais que uma organização possui para minimizar ameaças ou aproveitar oportunidades que possam influenciar os objetivos organizacionais.

Tabela 3 - Definição de Gestão de Riscos

Organização	Conceito de Gestão de Riscos
Business Continuity Institute (BCI, 2017)	Cultura, processos e estruturas implementadas para gerenciar efetivamente oportunidades potenciais e efeitos adversos.
Controladoria Geral da União (CGU, 2018)	Processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais. A gestão de riscos é composta por arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente.
COSO (COSO, 2017)	Estratégia sólida, capaz de identificar, avaliar e administrar riscos. É a cultura, as competências e as práticas que as organizações integram à definição e à execução da estratégia, com o objetivo de gerenciar o risco na criação, na preservação e na realização de valor.
Ferma (FERMA, 2003)	Elemento central na gestão da estratégia de qualquer organização. É o processo através do qual as organizações analisam metodicamente os riscos inerentes às respectivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades.
HM Treasury (HMT, 2004)	Todos os processos envolvidos na identificação, avaliação e julgamento de riscos, atribuição de propriedade, tomada de ações para mitigá-los ou antecipá-los, além de monitorar e revisar o progresso.
Instituto Brasileiro de Governança Corporativa (IBGC, 2017)	Sistema intrínseco ao planejamento estratégico de negócios, composto por processos contínuos e estruturados, desenhados para identificar e responder eventos que possam afetar os objetivos da organização, e por uma estrutura de governança corporativa, responsável por manter esse sistema vivo e em funcionamento.
Institute of Risk Management (IRM, 2012)	Processo que visa ajudar as organizações a entender, avaliar e agir sobre todos os seus riscos, com vistas a aumentar a probabilidade de sucesso e reduzir falhas.

ISO Guide 73 (2005) / ISO 31000 (2009,2018)	Atividades coordenadas para direcionar e controlar uma organização no que refere-se a riscos.
M_o_R-OGC (2010)	Aplicação sistemática de princípios, abordagens e processos para as tarefas de identificação e avaliação de riscos, seguidas de planejamento e implantação de respostas aos riscos. Processo de identificação e controle de exposição da organização ao risco.
PMI (2013, 2017)	Inclui os processos de planejamento, identificação, análise, respostas e controle de riscos de um projeto. Os objetivos do gerenciamento dos riscos do projeto são aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.
Tribunal de Contas da União (2018c)	Conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos de forma a aumentar a capacidade da organização de lidar com as incertezas.
*HMG - The Orange Book (*2019)	Todos os processos que envolvem a identificação, a avaliação, a decisão quanto a tratamento de riscos, a definição de responsáveis e a tomada de ações para mitigar ou antecipar os riscos, bem como monitorar e revisar o progresso dessas atividades. É o processo que visa conferir razoável segurança quanto ao alcance dos objetivos.

Conforme pode ser verificado na tabela 3 as organizações definem a gestão de riscos como sendo uma “estratégia”, “processo” ou um “conjunto de atividades” de forma a auxiliar o gestor a identificar, analisar, avaliar, monitorar, tratar, documentar e relatar riscos dentro da organização. A partir das definições apresentadas na tabela 3 é concebível compreender que os modelos e normas apresentam o conceito da gestão de riscos de forma semelhante com pequenas diferenças em relação às atividades realizadas.

Enquanto o COSO trata a gestão de riscos como sendo uma estratégia, IRM, CGU, HMT, HMG abordam como sendo um processo, as ISOS e TCU conceituam como sendo atividades coordenadas. Neste sentido, a gestão de riscos pode ser compreendida como o processo para identificar, mensurar, avaliar, monitorar, documentar, reportar, controlar e mitigar riscos envolvendo recursos humanos, materiais e financeiros, com o objetivo de reduzir e minimizar os impactos negativos, gerando oportunidades de economia ou ganho para a corporação.

Em razão da complexidade do processo de gestão de riscos, ao longo dos anos surgiram leis, normativas, modelos, guias, manuais e processos de forma a facilitar o controle das incertezas dentro da organização. Embora tem-se modelos

publicados desde 1992 até hoje as organizações públicas têm dificuldade de realizar o monitoramento e controle efetivo de riscos (TCU, 2018f; 2018g).

Dentro do panorama apresentado, a figura 2 demonstra que a preocupação com a gestão de riscos é antiga. Novos *frameworks*, atualizações de normas, guias, manuais, metodologias, roteiros e legislações sobre este tema surgem todos os anos.

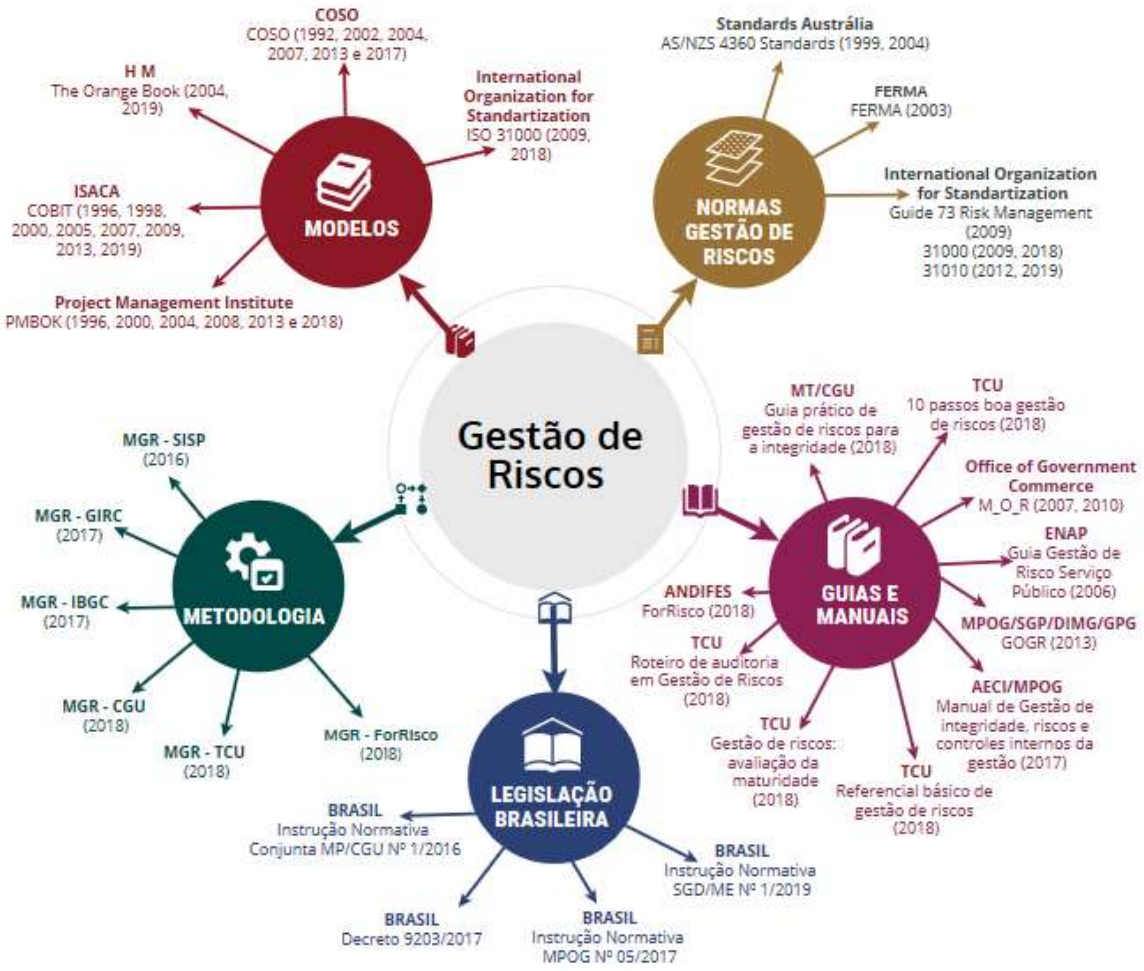


Figura 2 - Panorama da Gestão de Riscos

A partir da figura 2 verifica-se que algumas abordagens de gestão de riscos evoluíram ao longo dos anos. Dentre elas destacam a Norma ISO 31000 (2009, 2018) e os *frameworks* de gestão de riscos COSO (1992, 2002, 2004, 2007, 2013 e 2017), COBIT (1996, 1998, 2000, 2005, 2007, 2009, 2012, 2019), *HMT* (2004), HMG (2019) e PMI (1996, 2000, 2004, 2008, 2013, 2018).

Estas abordagens são referências importantes em gestão de riscos e se aderem ao contexto da Administração Pública Federal Brasileira. Por isso, serão abordadas na seção 2.3.

2.2.2 Riscos no Setor Público

Segundo o TCU (2018c), a sociedade anseia por uma administração pública ágil, transparente e eficiente, capaz de implementar políticas e programas de governo que entreguem serviços com maior eficácia para a população. Todavia, algumas vezes essas expectativas são frustradas e, ao se analisar as causas por trás das dificuldades em corresponder a estes anseios, depara-se não apenas com restrições orçamentárias e deficiências de diferentes naturezas, mas principalmente com a baixa capacidade das organizações públicas para lidar com riscos.

No âmbito governamental, os riscos podem ter impactos de grande escala, uma vez que podem envolver altos recursos financeiros. A capacidade de antevê-los, identificá-los, analisá-los e elaborar um planejamento de respostas contundente, depende significativamente da percepção das pessoas, que precisam desenvolver um olhar aguçado sobre o contexto ou realidade em que se inserem (ENAP, 2019).

Dentro do panorama apresentado no documento *The Orange Book* (HMG, 2019) é descrito que as organizações do setor público não podem ser avessas ao risco e serem bem sucedidas. O risco é inerente a tudo o que a organização faz para fornecer serviços de alta qualidade, por isso deve ser gerenciado.

Neste sentido, a gestão de riscos no contexto governamental deve ser eficiente de forma a gerenciar ameaças e oportunidades. Ela deve ser parte integrante do processo de tomada de decisão informada, no início da política ou do projeto até a prestação diária de serviços públicos à sociedade.

Quando a gestão de riscos é realizada de maneira estruturada, ela auxilia o direcionamento estratégico e a tomada de decisão de forma que os objetivos organizacionais sejam alcançados através da oferta de serviços públicos de qualidade. Consequentemente, aumenta a confiança dos cidadãos nas

organizações públicas, além de prevenir perdas e auxiliar na gestão de incidentes e no atendimento de requisitos legais e regulamentares.

Para Vieira (2019) apud TCU (2017), ao executar a gestão de riscos de forma adequada, as organizações geram benefícios que impactam diretamente nos cidadãos e outras partes interessadas. O gerenciamento de riscos viabiliza o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos, aumenta o grau de eficiência no processo de criação, proteção e entrega de valor público, otimiza a conformidade e o desempenho, eleva os resultados entregues à sociedade.

No âmbito público, a gestão de riscos já vem sendo adotada por vários órgãos governamentais ao redor do mundo (BERMEJO et al., 2019). No cenário brasileiro já é uma realidade no arcabouço normativo, ainda que sua efetiva adoção permaneça sendo um desafio (CGU, 2018b). No Brasil, o marco regulatório que orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança é a Instrução Normativa Conjunta MP/CGU Nº 1, de 10 de maio 2016 (BRASIL, 2016).

Em 2017, o Decreto Nº 9.203/2017, tornou obrigatória adoção da gestão de riscos no âmbito do Poder Executivo Federal (BRASIL, 2017). A partir desta publicação, todo gestor público ciente de suas responsabilidades, ao tomar decisões para atingir os objetivos estabelecidos para a sua organização, deve adotar atividades estruturadas e formalizadas para esse fim (CGU, 2018).

Dentro do panorama apresentado, a conscientização da necessidade de administração dos riscos potenciais é, hoje, uma questão de competitividade e sobrevivência para as organizações públicas. O desafio da governança nas organizações públicas é determinar quanto risco aceitar na busca do melhor valor para os cidadãos e outras partes interessadas (PARDINI, 2019).

Isto significa prestar o serviço de interesse público da melhor maneira possível, equilibrando riscos e benefícios (INTOSAI, 2007). Com isso, as organizações públicas terão condições de realizar a transformação digital de forma eficiente e segura, prestando serviços de qualidade, conforme a sociedade espera.

2.2.3 Gestão de Riscos em Aquisições de TIC

A gestão de riscos em TIC no setor público, segundo o TCU (2018), tem como finalidade evitar desperdício de recursos públicos e aumentar a efetividade dos processos. A adoção desta prática em aquisições de TIC, reflete o desejo da sociedade por serviços mais eficientes, ágeis e seguros através do aprimoramento dos controles que minimizam as incertezas e maximizam as oportunidades.

Considerando a complexidade dos projetos de Tecnologia da Informação e Comunicação e a rigidez dos contratos celebrados pela Administração Pública, a gestão de riscos atua como importante subsídio para o êxito das aquisições de TIC. Ela permite antever possíveis empecilhos no decorrer da contratação, proporciona melhor confiança entre as partes envolvidas, sejam elas internas ou externas, e resguarda o órgão quanto aos seus deveres perante o monitoramento da execução do contrato (PIRES, 2016).

Segundo o PMI (2013) para ter êxito, a organização deve estar comprometida com uma abordagem proativa e consistente do gerenciamento dos riscos durante todo o projeto. É preciso fazer uma escolha consciente em todos os níveis da organização para identificar ativamente e buscar a gestão eficaz dos riscos durante o ciclo de vida do projeto.

Os riscos do projeto podem existir no momento em que o projeto é iniciado. Avançar um projeto sem focar a administração dos riscos de forma proativa pode causar mais problemas, surgidos em virtude de ameaças não gerenciadas (PMI, 2013).

Para que a administração de riscos seja implantada de forma eficiente no processo de aquisições de TI visando o alcance dos objetivos organizacionais é fundamental que seja embasada em modelos, normas e leis sobre gestão de riscos. O gerenciamento de riscos deve ser realizado em harmonia com a política de gestão de riscos do órgão prevista na Instrução Normativa Conjunta MP/CGU Nº 1, de 10 de maio de 2016 (BRASIL, 2016).

Segundo a Instrução Normativa SGD/ME Nº 1/2019, no artigo 8, parágrafo 1, as atividades de gerenciamento de riscos devem ser realizadas durante todas as fases do processo de contratação, observando o disposto no artigo 38 (BRASIL,

2019b). A Instrução Normativa MPOG Nº 5/2017, trata sobre a obrigatoriedade do gerenciamento de riscos no artigo 20. O artigo 25 detalhada as atividades que compõem o processo de gestão de riscos.

De acordo com as informações divulgadas pelo TCU (2018f) diversas instituições ainda estão no estágio inicial ou inexpressivo da capacidade de gerir riscos em aquisições, uma vez que não gerenciam riscos críticos da área de contratações, tem dificuldade em realizar o monitoramento do desempenho da gestão de contratações, a equipe não está capacitada para gerir o contrato, o clima organizacional nem sempre é favorável a gestão de riscos e a organização não definiu o processo de trabalho para planejamento de cada uma das contratações (TCU, 2018g).

Provavelmente a baixa capacidade de gerir riscos relacionados ao processo de aquisições de TIC esteja vinculada à falta de procedimentos sistematizados para realizar o monitoramento e controle contínuo de riscos de maneira prática, documentada e transparente para a sociedade, de forma que as lições aprendidas possam ser aproveitadas para futuros processos aquisitivos. Um catálogo de riscos com controles a serem aplicados pode ser uma contribuição para agilizar o processo de identificação, avaliação e tratamento de riscos em aquisições de TIC.

2.2.4 Riscos em Aquisições de TIC

Existem diversos riscos envolvendo as fases do processo de aquisições de TI. A tabela 4 detalha exemplos de riscos existentes em contratações de TIC. Os riscos foram compilados a partir de TCU (2013) e Nobre (2017).

Tabela 4 – Riscos Relacionados a Aquisições de TIC

Fase	Categoria	Risco
Planejamento da Contratação	Orçamento/Financeiro	Coleta insuficiente de preços, levando a estimativas inadequadas.
	Organização	Imprecisão do objeto, de modo que a natureza, as quantidades ou o prazo não fiquem claros, levando a contratação que não atenda à necessidade do órgão.
	TI	A análise de risco ser otimista, desconsiderando riscos relevantes.
	Organização	Falta de participação da área requisitante da solução de TI, especialmente com relação à construção e à manutenção da solução (e.g.

		desenvolvimento de novos módulos e elaboração de novos relatórios de sistema de informação), levando à execução inadequada do objeto.
Seleção do Fornecedor	TI	Dificuldade dos atores envolvidos de justificar a adequação das estimativas de preço da contratação quando questionados.
Gestão do Contrato	Organização	Não alcance dos resultados pretendidos com a contratação.
	Organização	Falta de servidores na área de TI com domínio do processo de gestão contratual, levando a gestão de contrato deficiente.
	Organização	Sobrecarga dos servidores responsáveis por atividades do processo de gestão dos contratos, levando à execução inadequada desse processo.
	Organização	Atraso no alcance dos resultados pretendidos com a contratação devido a intempestividade da adequação do ambiente do órgão (uma nova solução pode demandar o aumento da velocidade da rede interna do órgão e dos links de acesso à internet e essas mudanças ocorrerem somente após a implantação da solução).
	Financeiro	Pagamentos indevidos por serviços parcialmente executados ou não executados.
	Financeiro	Pagamentos superfaturados, isto é, com valores acima dos previstos no contrato.
	Conformidade	Contratação direta (dispensa ou inexigibilidade) sem que haja modelos adequados de execução do objeto e de gestão do contrato.

A tabela 4 apresenta exemplos de riscos existentes no processo de aquisição de TI. Os riscos foram classificados por fase e categoria de forma a apresentá-los de forma didática e estruturada.

Diante do exposto, utilizar boas práticas e padrões definidos em modelos reconhecidos no mercado é uma maneira eficaz de estabelecer uma abordagem sistemática e estruturada para a gestão de riscos (TCU, 2018c). Dentro da perspectiva apresentada, optou-se por detalhar neste estudo, apenas as abordagens, normas e metodologias mais recentes, tendo em vista que já são referências utilizadas pelos setores público e privado.

2.3 ABORDAGENS SOBRE GESTÃO DE RISCOS

Segundo Bermejo et al. (2019), no início do Século XXI, houve a consolidação e disseminação de práticas de gestão de riscos corporativo. Entre as publicações que

se tornaram referências internacionais no tema tem-se: *The Orange Book (2004, 2019)*, lei *Sarbanes-Oxley* (2002), COSO (1992, 2002, 2004, 2007, 2013 e 2017), COBIT (1996, 2007, 2012, 2019), AS/NZS 4360 (2004), ISO 31000 (2009, 2018) e a ISO 31010 (2009, 2019). Nesta seção serão abordados modelos e normas sobre gerenciamento de riscos considerados como referências atuais sobre esta temática.

2.3.1 COSO

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) em 2001 publicou a obra *Internal Control – Integrated Framework* para ajudar empresas e outras organizações a avaliar e aperfeiçoar seus sistemas de controle interno (COSO, 2007). Desde então, a referida estrutura foi incorporada em políticas, normas e regulamentos adotados por várias organizações para controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos.

O *framework* COSO tem por finalidade fornecer elementos para o gerenciamento de riscos corporativo nas diversas dimensões do processo de gestão. Sua abordagem integra a gestão de riscos com desempenho, explorando como a identificação e avaliação de riscos podem impactar a implementação da estratégia e o alcance dos objetivos de negócios (BRASILIANO, 2018).

O COSO define e conceitua componentes e princípios, e fornece orientação para todos os níveis de gerenciamento de riscos corporativos, envolvidos na concepção, implementação e operacionalização da gestão de riscos. Este *framework* oferece orientação sobre como integrar o controle de riscos corporativos incluindo riscos à definição de estratégias e atividades cotidianas, incorporando-os a cultura, capacidades e práticas de uma organização e promove decisões melhores e mais assertivas (COSO, 2017).

Em 2017 foi lançado o COSO ERM versão 2017, uma versão atualizada da *Enterprise Risk Management - Integrated Framework*, de 2004 (COSO, 2004). Esta abordagem trata a necessidade das organizações melhorarem o gerenciamento de riscos para atender às demandas de um ambiente de negócios em evolução (COSO, 2017).

A estrutura do COSO ERM versão 2017 é organizada e estabelecida em cinco componentes: governança e cultura, estratégia e definição dos objetivos, desempenho, análise e revisão, informação, comunicação e relatórios que se combinam. Dessa forma, o processo de gestão de riscos no COSO ERM versão 2017 envolve principalmente estratégia e definição de objetivos, performance e análise e revisão (COSO, 2017). Este processo está detalhado na figura 3.

Figura 3 - Gestão de Riscos - COSO

O processo de gerenciamento de riscos do *framework* COSO ERM versão 2017 apresentado na figura 3 envolve 20 princípios. Dentre eles, 5 (cinco) princípios são semelhantes aos demais modelos de gestão de riscos: identifica o risco, avalia a severidade do risco, prioriza os riscos, implementa respostas aos riscos e adota uma visão de portfólio (COSO, 2017).

2.3.2 COBIT

O *framework Control Objectives for Information and Related Technologies* (COBIT) foi concebido pela *Information Systems Audit and Control Association* (ISACA) em 1996. Esta abordagem surgiu como um modelo para auditoria e controles de processos de TI, com foco nos objetivos de controle para ajudar a comunidade de auditoria financeira a lidar com ambientes relacionados a TI (ISACA, 2013). Na APF, o COBIT versão 4.1 e 5 são utilizados como referência na construção de acórdãos

para a regulamentação de princípios e diretrizes, definição de processos e estabelecimento de estruturas organizacionais do TCU.

Para ISACA (2013), o COBIT é um *framework* de boas práticas para a governança e gestão corporativa de TI que concentra na implementação, medição, fiscalização e melhoria dos controles dos processos de TI. Este modelo possui alinhamento com os modelos COSO, COSO ERM, ISO 9000, ISO 31000, ISO 38500, ITIL, ISO series 27000, TOGAF, PMBOK, PRINCE2 e CMMI. Uma diferença entre o COBIT e outros *frameworks* é que ele foca especificamente em segurança, gerenciamento de riscos e governança de informações.

A estrutura do COBIT 5 é composta por cinco domínios, 37 processos e 210 pontos de controle. Em relação a governança tem o domínio avaliar, dirigir e monitorar. Em gestão tem-se os domínios: alinhar, planejar e organizar; construir, adquirir e implementar; entregar, serviço e suporte; e monitorar, avaliar e analisar (ISACA, 2013). O processo de gerenciamento de riscos é tratado no domínio alinhar, planejar e organizar (APO-12) e está apresentado na figura 4.

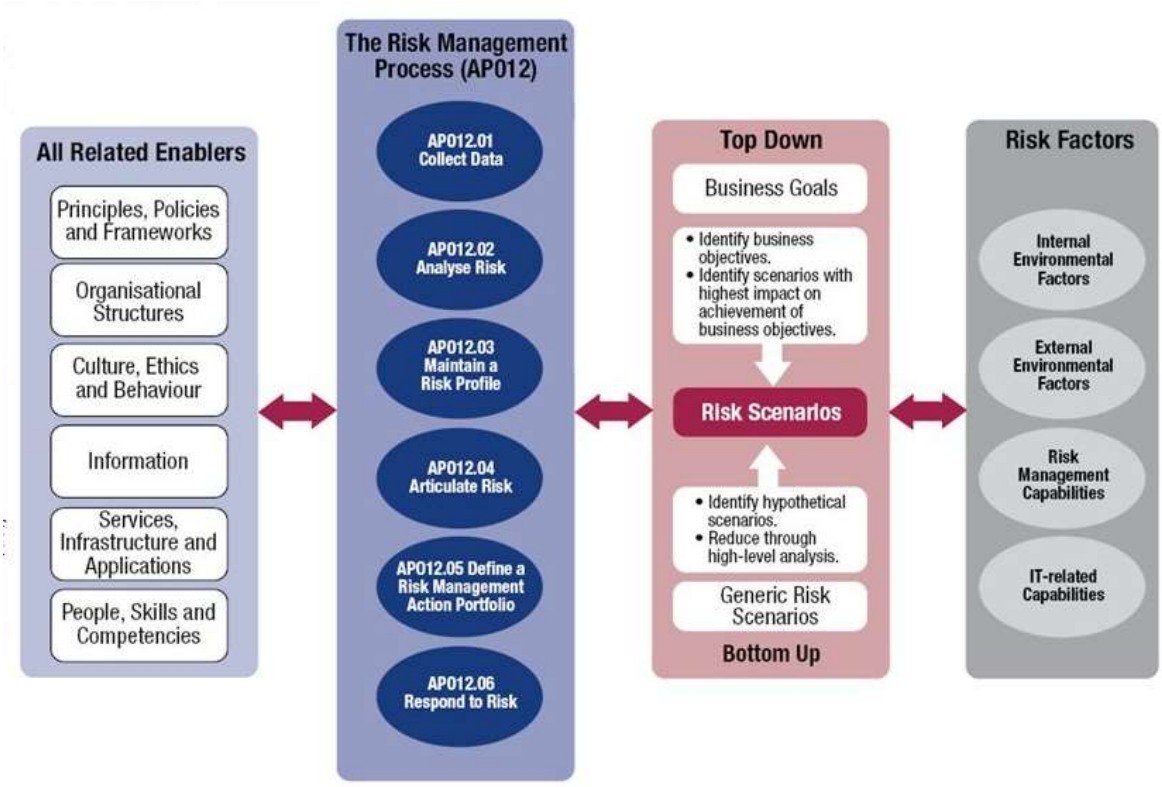


Figura 4 - Gestão de Riscos - COBIT 5 for Risk

O processo de gerenciamento de riscos do COBIT (APO-12) apresentado na figura 4 é responsável por identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva (ISACA, 2013). Ele é composto por coletar dados, analisar risco, manter um perfil de risco, articular o risco, definir um portfólio de ações para gerenciamento de risco e responder ao risco.

Para implementar o COBIT deve-se: compreender o contexto e a estratégia da empresa, determinar o escopo inicial do sistema de governança, refiná-lo e concluir o seu desenho (ISACA, 2013). Com isso, a área de TI terá condições de ter o controle eficiente de seus processos organizacionais.

2.3.3 The Orange Book

A primeira versão do *framework The Orange Book Management of Risk - Principles and Concepts foi* produzida e publicada pelo HM *Treasury* do Governo Britânico em 2001 (HMT, 2004). O *The Orange Book* é um conjunto de regras para gerenciamento de riscos em organizações governamentais compatível com padrões internacionais de gerenciamento de riscos COSO e ISO 31000.

The Orange Book é uma abordagem que propõe à organização o gerenciamento de riscos em diversos níveis, como, por exemplo, no nível estratégico, de programas e de projetos ou operações e atividades. A sua estrutura suporta a identificação consistente e robusta e o gerenciamento de oportunidades e riscos dentro dos níveis desejados em toda a organização, apoiando a abertura, o desafio, a inovação e a excelência na realização dos objetivos (HMG, 2019).

A metodologia de gestão de riscos deste *framework* engloba princípios, abordagens e processos em um conjunto de passos inter-relacionados para o gerenciamento de riscos em organizações (BERMEJO et al., 2019). A versão atual deste modelo foi divulgada em 2019.

O *framework The Orange Book* considera a gestão de riscos como sendo todos os processos que envolvem a identificação, a avaliação, a decisão quanto a tratamento de riscos, a definição de responsáveis e a tomada de ações para mitigar

ou antecipar os riscos, bem como monitorar e revisar o progresso dessas atividades (HMG, 2019). A figura 5 apresenta o processo de gestão de risco proposto pelo *The Orange Book.*

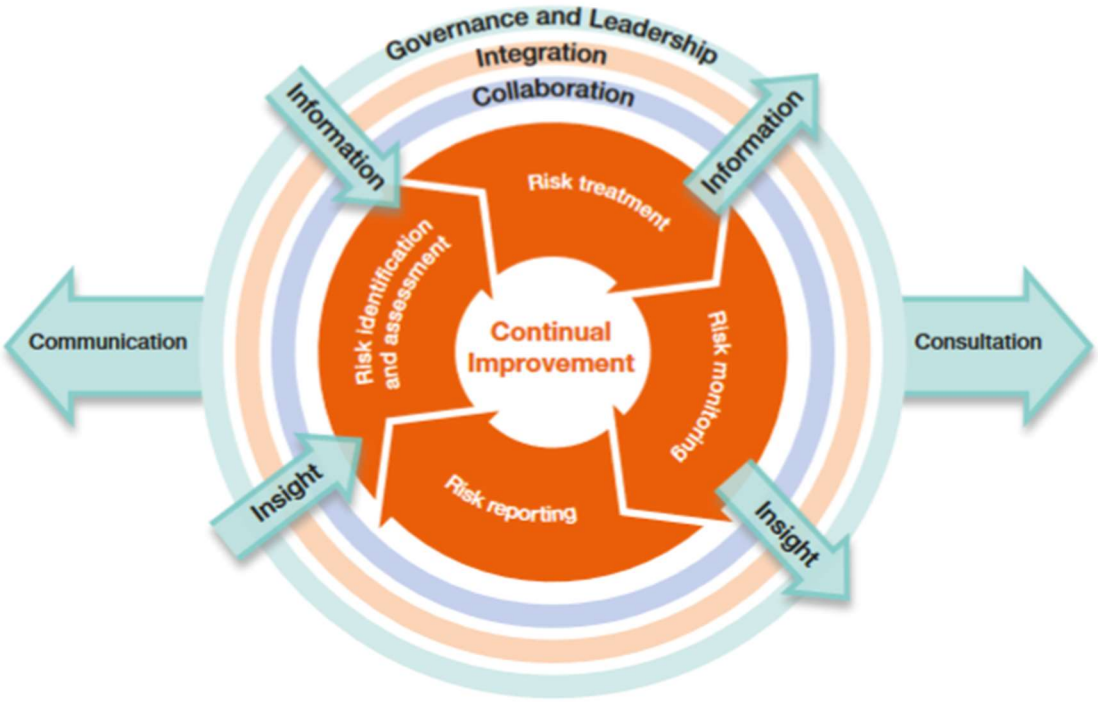


Figura 5 - Gestão de Riscos - The Orange Book

O processo de gerenciamento de riscos apresentado na figura 5 é composto por identificação e avaliação de riscos, tratamento de riscos, monitoramento de riscos e relatórios de riscos (*HMG*, 2019). Esta abordagem trata a gestão de riscos de forma abrangente podendo ser utilizado por qualquer tipo de organização.

O *The Orange* Book é apoiado por técnicas e ferramentas para identificação, avaliação e tratamento de riscos assim como o *framework* apresentado pela ISO 31000. Dentre elas podem ser citadas: matriz de risco (probabilidade x impacto), auto avaliação de risco, gestão de relato, estrutura de avaliação de gestão de riscos, análise de SWOT, matriz de probabilidade e consequência, lista de verificação, lista de resposta, diagrama de causa e efeito, técnicas de grupo, Delphi, questionários, entrevistas, descrições de risco, mapa de risco, árvore de decisão, resposta ao risco (HMT, 2004; OGC, 2010).

Além das técnicas e ferramentas citadas o *The Orange Book* utiliza um conjunto de documentos norteadores nas definições de como serão conduzidas as

ações, o modo como serão comunicadas, geridas e melhoradas ao longo do tempo. Dentre os documentos tem-se: política, guia de processos, estratégia, registro de risco, registro da questão, plano de melhoria para gestão de riscos, plano de comunicação do risco, plano de resposta ao risco, plano de progresso do tratamento do risco (OGC, 2010).

2.3.4 ISO Série 31000

A norma ISO 31000: gestão de riscos (princípios e diretrizes) surgiu em 2009 criada e divulgada pela *International Organization for Standardization.* A ISO 31000 busca definir e padronizar conceitos e processos de gerenciamento de riscos através de princípios e diretrizes em gestão de riscos que podem ser adotados por diferentes organizações nas atividades de decisão estratégica, operação, processo, função, projeto, serviço e avaliação de riscos (ISO, 2018).

Esta abordagem surgiu de forma a atender a necessidade de harmonizar padrões, regulamentações e *frameworks* publicados anteriormente e que de alguma forma estão relacionados com a gestão de riscos (BRASILIANO, 2018). A norma ISO 31000 promete melhorar o desempenho, encoraja a inovação e apoia o alcance de objetivos (ISO, 2018).

O modelo de gestão de riscos na norma ISSO 31000 pode ser aplicado a vários tipos de riscos ligados aos diferentes setores da organização, tais como: financeiro, saúde e meio ambiente, tecnologia da informação, segurança empresarial, seguros, e de projetos, entre outros, incluindo a visão moderna de que risco também é oportunidade (ISO, 2018). Esta norma propõe que o processo de gestão de riscos seja parte integrante da gestão corporativa, incorporado na cultura e nas práticas da organização e que seja adaptado aos processos de negócio (ISO, 2018).

A ISO 31000 (2018) apresenta um conjunto de etapas contendo os princípios, a estratégia e o processo de avaliação de riscos de forma a gerenciar riscos de maneira consistente. O processo de gestão de riscos apresentado pela norma elenca as técnicas e ferramentas para permitir que se busque uma avaliação sistemática dos riscos.

Dentre as ferramentas e técnicas recomendadas pela ISO série 31000 podem ser citadas: *brainstorming*, entrevistas estruturadas ou semiestruturadas, Delphi, listas de verificação, análise de preliminar de perigos, análise de cenários, análise de causa-raiz, análise de causa e consequência, análise de causa e efeito, árvore de decisão, análise de *bow-tie*, índices de riscos, matriz de probabilidade/consequência. A figura 6 apresenta o *framework* de gerenciamento de riscos contido na versão publicada em 2018 (ISO, 2018).

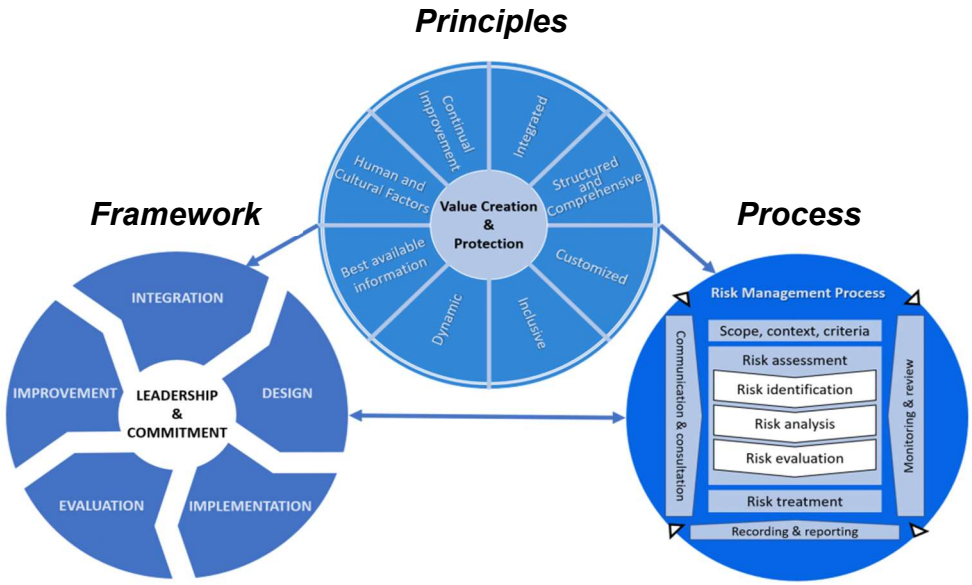


Figura 6 - Gestão de Riscos - ISO 31000

O *framework* de gestão de riscos proposto pela norma ISO 31000 apresentado na figura 6 é composto por estrutura, princípios e processo. O processo de gerenciamento de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto, processo de avaliação de riscos (identificação, análise e avaliação), tratamento de riscos, monitoramento, análise crítica, registro e relato de riscos. É um processo genérico que pode ser adaptado para qualquer tipo de organização (ISO, 2018).

De forma complementar a norma ISO 31000 (informações básicas, princípios e diretrizes para a implementação da gestão de riscos), a ISO 31010 (técnicas para o processo de avaliação de riscos) fornece orientações sobre a seleção e a aplicação de técnicas sistemáticas para o processo de avaliação de riscos, contribuindo com as atividades de gestão da organização. De acordo com o

processo de avaliação dos riscos, ao empregar as técnicas e ferramentas propostas na ISO 31010, é possível compreender melhor os riscos e angariar informações relevantes que auxiliam a tomada de decisão e o estabelecimento de priorizações para o tratamento dos riscos (ISO, 2019).

2.3.5 PMBOK

O *Project Management Body of Knowledge* (PMBOK) é um guia contendo boas práticas para o gerenciamento de projetos organizado pelo *Project Management Institute (PMI)*. Esta abordagem surgiu em 1996 e desde então a cada 4 anos uma nova edição é publicada (PMI, 2017).

PMBOK é considerado como um conjunto de conhecimentos de gerenciamento de projetos composto por 5 grupos de processos: iniciação, planejamento, execução, monitoramento e controle e encerramento. Este guia possui 10 áreas de conhecimento de gestão de projetos. São elas: integração, escopo, tempo, custo, qualidade, aquisição, recursos humanos, comunicações, riscos e partes interessadas (PMI, 2017).

A gestão de riscos nesta abordagem é realizado a partir da execução dos processos: planejar o gerenciamento de riscos, identificar os riscos, realizar a análise qualitativa dos riscos, realizar a análise quantitativa dos riscos, planejar as respostas aos riscos, implementar respostas aos riscos e monitorar os riscos, conforme apresenta a figura 7.

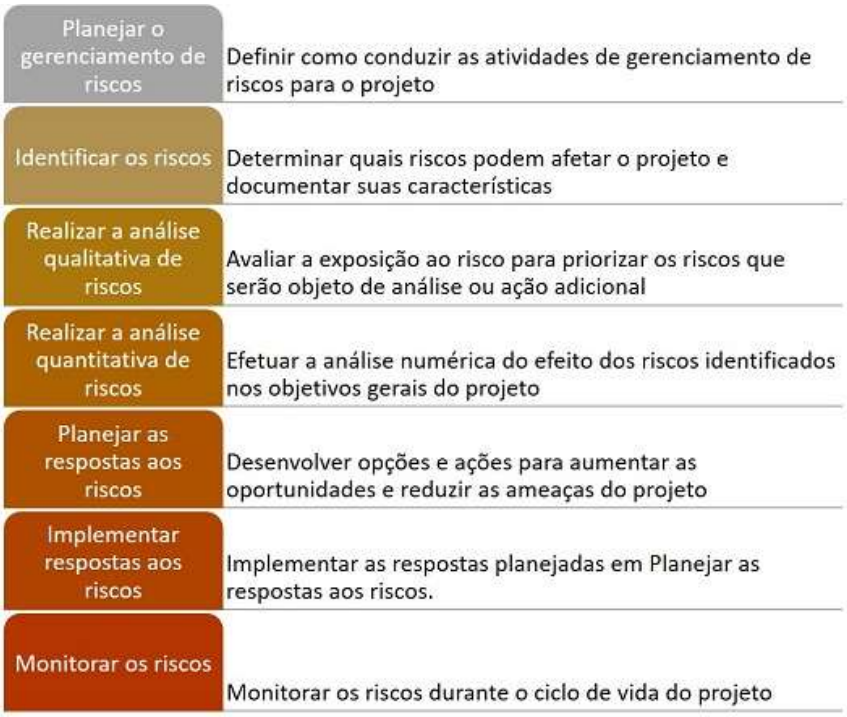


Figura 7 - Gestão de Riscos – PMBOK

A figura 7 mostra o processo de gerenciamento dos riscos do projeto proposto pelo PMBOK 6ª edição que inclui os processos de condução do planejamento, identificação, análise, planejamento de respostas, implementação de respostas e monitoramento dos riscos em um projeto. Para que um projeto tenha resultados satisfatórios, o PMI (2017) sugere que o projeto seja gerenciado do início ao fim. De acordo com esta abordagem a organização deve estar comprometida com uma abordagem proativa e consistente do gerenciamento de riscos durante todo o projeto (NOBRE, 2017).

2.4 METODOLOGIAS DE GESTÃO DE RISCOS NO SETOR PÚBLICO

As metodologias de gestão de riscos existentes no setor público geralmente são compostas por um conjunto de boas práticas e padrões definidos para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos que possam comprometer o desempenho da organização. Estas metodologias foram desenvolvidas em diferentes momentos e contextos, entretanto possuem diversas semelhanças entre si (BERMEJO et al., 2019). A figura 8 apresenta alguns exemplos de metodologias de gestão de riscos adotadas no setor público.

Figura 8 – Metodologias de Gestão de Riscos Utilizadas no Setor Público

A figura 8 apresenta metodologias de gestão de riscos desenvolvidas por instituições públicas brasileiras nos últimos 5 anos. A próxima seção descreverá suas abordagens, técnicas, ferramentas, processos, atividades, tarefas e artefatos. O conhecimento sobre as práticas adotadas em cada uma delas pode auxiliar na construção de uma metodologia específica para gerenciamento de riscos em aquisições de TIC.

2.4.1 MGR-SISP

A metodologia de gestão de riscos de segurança da informação e comunicação do SISP (MGR-SISP) foi criada em 2016 pelo Ministério do Planejamento, Desenvolvimento e Gestão, conforme a Instrução Normativa INC CGU/MP Nº 1/2016 (Brasil, 2016). A MGR-SISP visa padronizar e sistematizar a gestão de riscos de segurança da informação e comunicação na Administração Pública Federal (MPOG, 2016).

Para o desenvolvimento da MGR-SISP buscou-se o respaldo de padrões, como ISO 31000 (2009), ISO/IEC 27005 (2011), *IT Grundschutz BSI Standard* 100-2 (2008) e NIST SP 800-39, (2011). A MGR-SISP traz contribuições em relação ao

contexto brasileiro, contendo referências a normativas e leis vigentes aplicadas à gestão de riscos e, ainda, por dispor de um conjunto de processos, atividades e tarefas de forma estruturada (BERMEJO et al., 2019).

MGR-SISP é compatível com iniciativas anteriores voltadas à segurança da Informação e comunicação na APF, como a Norma Complementar nº 04/IN01/DSIC/GSIPR, do Gabinete de Segurança Institucional da Presidência da República, publicada em 15 de fevereiro de 2013. Além desta normativa utiliza a Instrução Normativa Conjunta N° 1, de 10 de maio de 2016, publicada pela então Controladoria-Geral da União (CGU) e pelo Ministério do Planejamento, Orçamento e Gestão (BRASIL, 2016).

Para realizar a gestão de riscos, a MGR-SISP exige que sejam definidos os critérios para avaliar o nível dos riscos e para decidir sobre qual tratamento deve ser realizado (MPOG, 2016). A aplicação da MGR-SISP em organizações pode ser apoiada por uma ferramenta computacional, muito embora seja independente de quaisquer ferramentas. A figura 9 apresenta os sub processos que compõem o processo de gerenciamento de riscos desta abordagem.

Figura 9 - Processo de Gestão de Riscos MGR-SISP

A MGR-SISP é associada a um processo, composto por sub processos, que por sua vez são decompostos em atividades, e estas em tarefas. A figura 9 ilustra o processo subjacente à MGR-SISP destacando a execução sequencial dos 7 processos: estabelecer o contexto, identificar riscos, estimar riscos, avaliar riscos, tratar riscos, comunicar riscos e monitorar riscos. Além disso, possui um total de 65 tarefas agrupadas em 16 atividades organizadas nos 7 processos apresentados na figura 9 (MPOG, 2016).

Na MGR-SISP a identificação, estimativa e informações sobre riscos são agrupadas em um documento denominado mapa de risco. Para comunicar os riscos a MGR-SISP usa o plano de comunicação de riscos que traz o mapeamento de todos os envolvidos na análise de riscos, estabelece quais as responsabilidades de cada um e define pontos relacionados a comunicação (MPOG, 2016).

2.4.2 MGR-GIRC

A Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão (MGR-GIRC) surgiu em 2017 pelo Ministério de Planejamento, Desenvolvimento e Gestão (MPOG). A MGR-GIRC tem por finalidade orientar, sistematizar e padronizar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos das unidades do Ministério do Planejamento a partir do método de priorização de processos organizacionais, bem como instruir sobre o monitoramento e reporte (MPOG, 2017b).

A MGR-GIRC tem foco em manter a integridade dos processos organizacionais pelos gestores públicos que devem corresponder às expectativas da sociedade (MPOG, 2017b). A MGR-GIRC incorpora boas práticas reconhecidas, apresentando características da estrutura de componentes do COSO ERM (COSO, 2007).

Nesta metodologia de gestão de riscos estão descritas as premissas, conceitos, papéis e responsabilidades, taxonomia de eventos de riscos e lista de controles básicos. A MGR-GIRC é constituída de quatro pilares: ambiente de integridade; gestão de integridade, riscos e controles; instituição e conformidade de procedimentos de integridade; e informação, comunicação e o monitoramento.

Na MGR-GIRC é apresentado o método de priorização de processos organizacionais com o objetivo de estabelecer prioridades e definir prazos para gerenciamento de riscos, cujo escopo são os processos organizacionais. Esta metodologia é composta por 4 instrumentos: Política de Gestão de Integridade, Riscos e Controles Internos da Gestão; Instâncias de Supervisão; Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão; e Solução

Tecnológica (MPOG, 2017b). A figura 10 apresenta as etapas do processo de gerenciamento de riscos da MGR-GIRC.

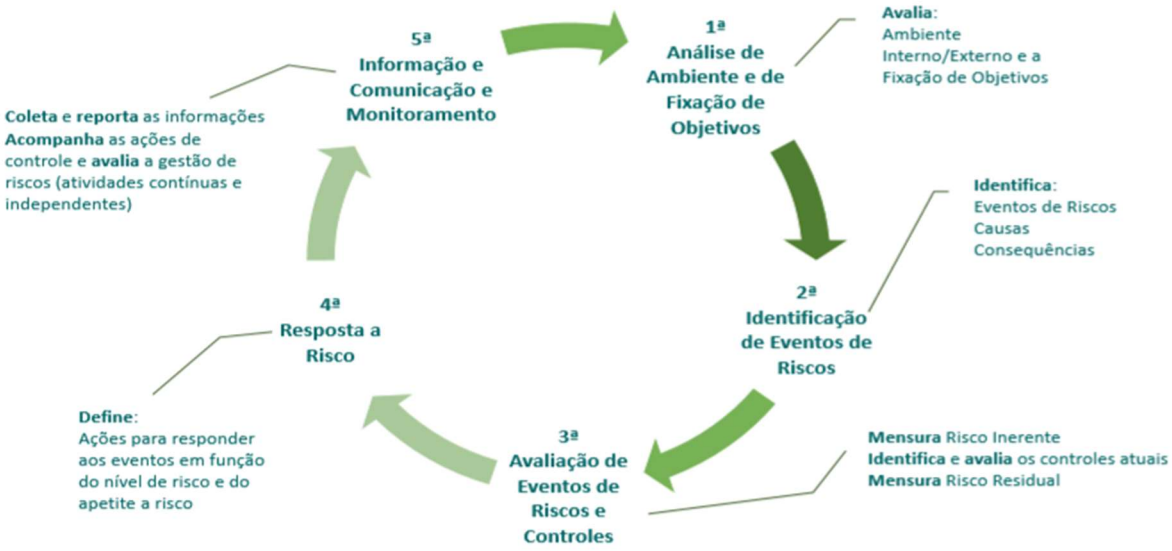


Figura 10 - Processo de Gestão de Riscos MGR-GIRC

A metodologia de gestão de riscos MGR-GIRC apresentada na figura 10 é composta por 5 etapas: análise de ambiente e fixação de objetivos, identificação de eventos de riscos, avaliação de eventos de riscos e controles, resposta a risco e informação, comunicação e monitoramento (MPOG, 2017b). Segundo esta abordagem, riscos e oportunidades mudam ao longo do tempo, portanto devem ser monitorados para que a organização possa realizar os ajustes necessários.

Na MGR-GIRC a identificação dos eventos é feita através da ferramenta chamada planilha documentadora. A análise de SWOT realiza a análise de ambiente e de fixação de objetivos identificando as forças e fraquezas e as possíveis influências do ambiente externo. Para registrar as informações coletadas nesta etapa a MGR-GRIC usa uma ferramenta tecnológica disponibilizada pela Assessoria Especial de Controles Internos do MPOG (MPOG, 2017b).

Para a identificação de eventos de riscos a MGR-GIRC utiliza as técnicas: questionários e *checklist*, *workshop* e *brainstorming*, inspeções e auditorias, fluxogramas, diagrama de causa e efeito, método *bow-tie* etc. O registro de riscos é feito no mapa de risco (MPOG, 2017b).

A avaliação de eventos de riscos e controles é registrada através da ferramenta planilha documentadora com auxílio da matriz de risco. Para implementar controles sobre riscos, esta abordagem possui o plano de implementação de controles disponibilizado através de formulário próprio para registro de ações necessárias para adequar os níveis de risco. (MPOG, 2017b).

Para que as instâncias de supervisão possam avaliar os controles implementados a MGR-GIRC usa os relatórios dos planos de implementação dos controles. A comunicação sobre os riscos é feita de acordo com os níveis de relacionamento estabelecidos no modelo de relacionamento envolvendo os níveis estratégico, tático e operacional (MPOG, 2017b).

Na MGR-GIRC o mapa de risco é a principal ferramenta para monitoramento do processo de gestão de integridade, risco e controle da unidade. Além desta ferramenta as unidades devem estabelecer indicadores de acompanhamento da implementação da metodologia de gestão de integridade, riscos e controles da gestão. Para comunicar sobre a gestão de integridade, risco e controles internos cada unidade deve desenvolver um relatório a cada seis meses para as partes interessadas (MPOG, 2017b).

2.4.3 MGR-CGU

A metodologia de gestão de riscos da Controladoria Geral da União (MGR-CGU) foi estabelecida em 2018 pelo Ministério da Transparência e Controladoria Geral da União. Ela apresenta os fundamentos, a estrutura de gestão de riscos com o objetivo de orientar as unidades a implementá-la em conformidade com a sua Política de Gestão de Riscos, instituída por meio da Portaria CGU Nº 915, de 12 de abril de 2017 (CGU, 2018).

A metodologia de gestão de riscos MGR-CGU objetiva estabelecer e estruturar as etapas necessárias para a operacionalização do controle de riscos por meio da definição de um processo de gerenciamento de riscos. Ela está alinhada aos principais *frameworks* do mercado (COSO, ISO 31000) e com a legislação relacionada à gestão de riscos (Decreto Nº 9.203, de 22 de novembro de 2017, IN CGU/MP Nº 1/2016).

A MGR-CGU apresenta detalhamento na identificação e classificação dos riscos, através de uma escala de probabilidade e impacto, priorização e formas de tratamento do risco (SOUZA, 2018). A figura 11 apresenta as etapas desta metodologia.

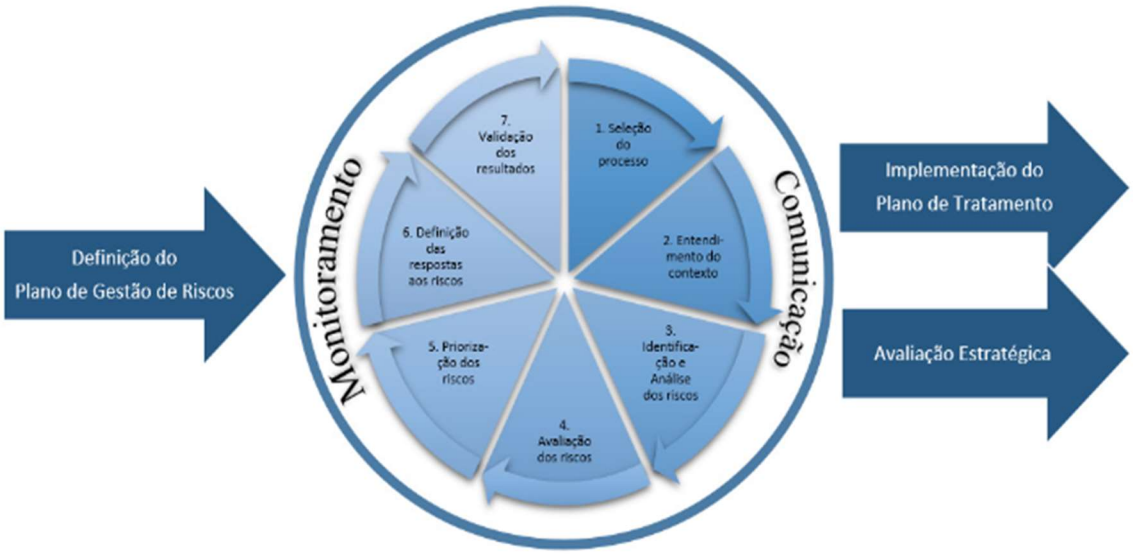


Figura 11 - Processo de Gestão de Riscos MGR-CGU

O processo de gestão de riscos da CGU apresentado na figura 11 é composto por 7 etapas: seleção do processo, entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos, definição de respostas aos riscos e validação dos resultados. A MGR-CGU disponibiliza o modelo de planilha de apoio ao processo de gerenciamento de riscos, plano de tratamento para o processo de elaboração dos critérios de avaliação estratégica (CGU, 2018). Além destes documentos, a MGR-CGU utiliza a matriz RACI como documento de comunicação durante a execução das etapas do processo de gestão de riscos da CGU (CGU, 2018).

Para identificar e analisar riscos, a MGR-CGU adota as técnicas de *brainstorming*, questionário e técnica Delphi. Para identificar os controles preventivos de riscos, são usadas lista de verificação (*checklist*), normativas e capacitação. Para comunicar e monitorar os riscos o Ministério da Transparência e Controladoria Geral da União utiliza a ferramenta painel de gestão de riscos (CGU, 2018c).

O monitoramento e a análise crítica da estrutura de gestão de riscos na MGR-CGU são constantes, por meio da comparação da gestão de riscos da CGU com bases normativas, *frameworks*, contextos de governo e da CGU, percepção de servidores, entre outros. Com o entendimento de que os resultados do monitoramento e da análise crítica podem impactar na estrutura é prevista uma revisão anual desses componentes (melhoria contínua da estrutura).

2.4.4 MGR-IBGC

A metodologia de gestão de riscos do Instituto Brasileiro de Gestão Corporativa (MGR-IBGC) foi divulgada em 2017 (IBGC, 2017). Ela foi desenvolvida para avaliação do nível de maturidade em gestão de riscos dentro de uma organização a partir da definição dos objetivos estratégicos e também do mapa de risco da organização.

Segundo Bermejo et al. (2019) ela surgiu no contexto das organizações privadas, entretanto adere ao setor público. Apesar de destinar-se primariamente a empresas com fins lucrativos, os conceitos e sugestões poderão ser utilizados também por entidades do primeiro e do terceiro setor.

Para Bermejo et al. (2019), a MGR-IBGC estabelece a política de responsabilidade da diretoria para avaliar quais riscos a organização pode ficar exposta, desenvolver procedimentos para administrá-los e avaliar, discutir e aprovar a política de riscos proposta pelo comitê executivo de riscos. Para aferir o nível de maturidade das organizações em relação a gestão de riscos esta abordagem faz a junção das dimensões (princípios) do *The Orange Book* (HMT, 2004) com a forma de medição e apresentação contidas na metodologia do IBGC (MPOG, 2017).

Este ajuste facilita o entendimento e permite a criação de planos de melhoria e outras ações. O processo de gestão de riscos da MGR-IBGC, apresentado na figura 12, consiste em identificar o grau de apetite a riscos da organização e as faixas de tolerância e desvios em relação aos níveis de riscos aceitáveis (BERMEJO et al., 2019).

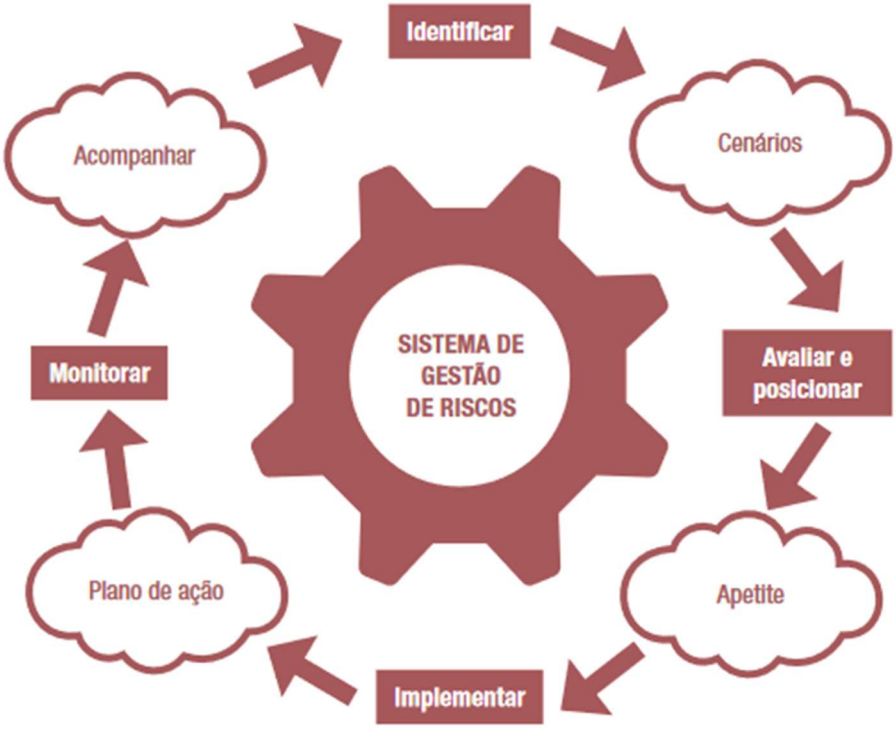


Figura 12 - Processo de Gestão de Riscos MGR-IBGC

O processo de gestão de riscos da MGR-IBGC mostrado na figura 12 é composto por 4 fases: identificar, avaliar e posicionar, implementar e monitorar. Para registrar os riscos esta metodologia utiliza as ferramentas de acompanhamento: mapa de risco e relatórios sumarizados (IBGC, 2017).

Na MGR-IBGC (2017) os riscos são categorizados através de uma matriz de risco que considera a origem dos eventos internos e externos à organização e a natureza dos riscos e sua tipificação. Para avaliar os riscos são considerados três aspectos: a probabilidade de ocorrência, a vulnerabilidade e o seu impacto. Nesta abordagem os riscos e suas categorias são documentados por meio do mapa de risco.

A MGR-IBGC (IBGC, 2017) utiliza relatórios periódicos de riscos e controles e opcionalmente sugere a adoção de indicadores-chave de riscos construídos a partir de intervalos de tolerância à perda. Também adota a elaboração de uma base de conhecimento de perdas relacionadas aos negócios de forma a auxiliar no direcionamento das decisões relacionadas aos riscos.

2.4.5 MGR-TCU

A metodologia de gestão de riscos do Tribunal de Contas União (MGR-TCU) foi publicada em seu manual de gestão de riscos em 2018 (TCU, 2018b). A MGR-TCU é baseada nas melhores práticas internacionais sobre o tema, COSO I (1992), COSO II (2004), COSO 2017 (2017), ISO 31000 (2009, 2018), *Orange Book* (UK, 2004 e 2009) e INTOSAI (Guias GOV 9100 e 9130).

A estratégia escolhida para implantação do gerenciamento de riscos é iterativa e baseia-se em ciclos sucessivos, com complexidade crescente. No TCU são objetos da gestão de riscos qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos do TCU. Unidades organizacionais também podem ser objeto do controle de riscos (TCU, 2018b).

O processo de gestão de riscos adotado pelo TCU é adaptado da norma ISO 31000. A avaliação de riscos estratégicos e alinhamento de objetivos segue o COSO 2017 (TCU, 2018b). A figura 13 apresenta as etapas que compõe o processo de gerenciamento de riscos proposto pela MGR-TCU.

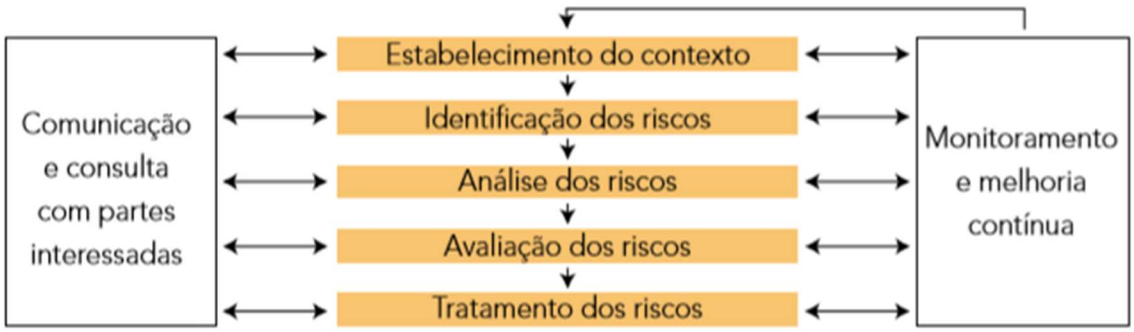


Figura 13 - Processo de Gestão de Riscos MGR-TCU

A metodologia de gestão do TCU (TCU, 2018b) apresentada na figura 13 é composta por 7 etapas: estabelecimento do contexto, identificação dos riscos, análise dos riscos, avaliação dos riscos, tratamento dos riscos, monitoramento e melhoria contínua, e comunicação e consulta com partes interessadas. A identificação dos riscos realizada nesta abordagem é feita através de oficinas de trabalho ou, dependendo do objeto, pelo próprio gestor do risco. Para a

identificação, análise, avaliação e resposta a risco são utilizadas as técnicas e ferramentas *brainstorming*, entrevistas, visitas técnicas, pesquisas entre outras instituições.

Para a análise de riscos a MGR-TCU utilizada a matriz de probabilidade x impacto com escalas predefinidas de 1 a 5. O registro de informações sobre riscos do projeto, atividade são realizadas através da tabela de gestão de riscos (TCU, 2018b).

O monitoramento das ações de tratamento de riscos, por sua vez envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. Os riscos são monitorados pelo gestor de riscos (TCU, 2018b).

2.4.6 MGR-ForRisco

A metodologia de gestão de riscos ForRisco (MGR-ForRisco) foi desenvolvida em 2018 com a participação de várias instituições federais de ensino superior, com o intuito de ser utilizada por qualquer organização pública (BERMEJO et al., 2019). A MGR-ForRisco é adequada ao contexto das instituições que compõem a APF em relação ao controle de riscos organizacionais, uma vez que já foi validada em algumas universidades federais com resultados satisfatórios (BERMEJO et al., 2019).

A MGR-ForRisco adota as boas práticas das abordagens de gerenciamento de riscos da ISO 31000, COSO ERM e *The Orange Book*. Ela traz no âmbito da gestão, um processo composto de 7 etapas fundamentais. São elas: a definição da política de gestão de riscos, o estabelecimento do contexto externo, a definição da estratégia para a gestão de riscos, o estabelecimento do contexto interno, a realização da gestão de riscos para as atividades, a reavaliação da política e o estabelecimento do nível de maturidade; e a avaliação da maturidade da organização (BERMEJO et al., 2019). O processo de gestão de riscos é apresentado na figura 14.

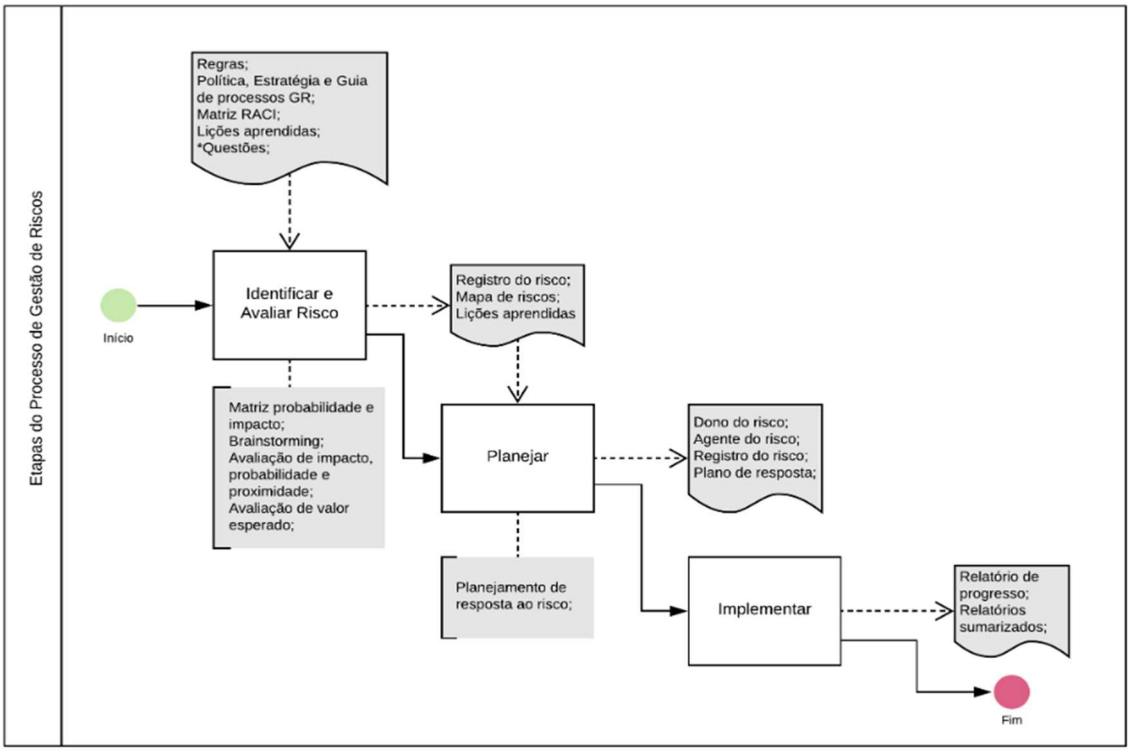


Figura 14 - Processo de Gestão de Riscos ForRisco

O processo de gestão de riscos proposto pela MGR-ForRisco é composto por 3 etapas: identificar e avaliar risco, planejar e implementar. A figura 14 apresenta as ferramentas e técnicas utilizadas. São elas: matriz RACI, lições aprendidas, registro de risco, mapa de risco, plano de resposta, relatório de progresso, comunicações e mensagens de alerta, árvore de decisão, *brainstorming*, análise de cenários por meio da matriz de SWOT e relatórios sumarizados.

Para monitorar, controlar e registrar os riscos relacionados às etapas apresentadas na figura 14, a MGR-ForRisco utiliza um software específico. Esta ferramenta tecnológica é fornecida de forma gratuita no site[1] do projeto sistema ForRisco (BERMEJO et al., 2019).

2.5 ANÁLISE CRÍTICA SOBRE GESTÃO DE RISCOS

No mercado existem diversas metodologias e ferramentas para a gestão de riscos que são aderentes ao cenário público e ao processo de aquisições de TIC. Observa-

[1] Site For Risco: http://www.forrisco.org/

se que as etapas/fases do processo de gerenciamento de riscos são basicamente as mesmas nas diversas abordagens, metodologias e normas existentes, com algumas variações terminológicas.

Através das publicações científicas e *gray literature* observa-se uma convergência entre abordagens de gestão de riscos para um entendimento que remete a um processo genérico de controle de riscos no qual destaca-se o entendimento do contexto, a identificação e avaliação de riscos, a elaboração e implementação de planos para tratamento de riscos (BERMEJO et al., 2019). Ao avaliar qual abordagem de gerenciamento de riscos se adequa ao contexto de aquisição de TIC no cenário brasileiro, deve-se observar aderência com o que está descrito na Instrução Normativa Conjunta MP/CGU Nº 1/2016 (BRASIL, 2016) prevista na Instrução Normativa SGD/ME Nº 1/2019 (BRASIL, 2019b).

As abordagens de gestão de riscos COSO e ISO 31000 se adaptam ao controle de riscos do processo de aquisição de TIC, uma vez que buscam definir e padronizar conceitos e processos do gerenciamento de riscos. As duas estruturas fornecem diretrizes genéricas para a administração de riscos que podem ser aplicadas para todo e qualquer tipo de organização (BERMEJO et al., 2019).

Alves (2017) afirma que a norma ISO 31000 e o *The Orange Book* não são concorrentes e sim complementares no que se refere a gestão de riscos. Para Dallas (2013) embora haja algumas diferenças entre a ISO 31000 e o *The Orange Book*, não existem áreas significativas em desarmonia quanto à abordagem geral e aos processos de gerenciamento de riscos, havendo uma ampla consistência entre seus princípios e diretrizes.

A fim de apoiar o processo de gestão de riscos referente a estrutura da ISO 31000, pode-se acrescentar com o uso da abordagem *The Orange Book*, tendo em vista a compatibilidade entre estes padrões e a ênfase no uso prático que o *The Orange Book* possui, fornecendo orientações detalhadas sobre como implementar o gerenciamento de riscos. Neste sentido, são adequadas para uso no processo de aquisição de TIC realizado pelas instituições públicas brasileiras.

Ao avaliar qual a melhor abordagem de gestão de riscos, deve ser levado em consideração o contexto interno e externo de cada Instituição. Observando o que recomenda a Instrução Normativa SGD/ME Nº 1/2019 (BRASIL, 2019b), as

metodologias MGR-SISP (MPOG, 2016), MGR-GIRC (MPOG, 2017), MGR-CGU (CGU, 2018), MGR-TCU (TCU, 2018b) e MGR-ForRisco (Bermejo et al., 2019), podem ser utilizadas para o controle de riscos do processo de aquisição de TIC em razão de estarem em harmonia com a Instrução Normativa MP/CGU Nº 1/2016 (BRASIL, 2016). Apenas a metodologia MGR-IBGC não está em conformidade com a legislação vigente, uma vez que sua abordagem é sobre medição do nível de maturidade em gestão de riscos. Entretanto, poderá ser usada de forma complementar (BERMEJO et al., 2019).

A partir das considerações apresentadas, é possível observar ao longo dos anos uma evolução do foco nas abordagens de gerenciamento de riscos, bem como um conjunto abrangente de técnicas e ferramentas para apoio aos gestores na condução dos riscos na organização em todos os *frameworks e metodologias* (BERMEJO et al., 2019*)*. Vale frisar que várias instituições públicas desenvolveram suas próprias metodologias de gestão de riscos, de acordo com seus contextos e particularidades.

Geralmente, as organizações utilizam as abordagens apresentadas nesta seção como modelo para construção de sua política, estrutura, estratégia e processo de gestão de riscos. Normalmente as instituições públicas brasileiras optam por desenvolver suas próprias metodologias para gerenciamento de riscos de acordo com seu contexto interno e externo, suas necessidades e objetivos organizacionais.

3 METODOLOGIA

O capítulo apresenta a caracterização da pesquisa, o método para a condução deste estudo, como foi conduzida a investigação, as técnicas utilizadas para coleta, análise e avaliação dos dados e os procedimentos metodológicos adotados. Por fim, detalha como foi realizada a revisão bibliográfica.

3.1 CARACTERIZAÇÃO DA PESQUISA

A finalidade da pesquisa segundo Barros e Lehfeld (2007) é resolver problemas e solucionar dúvidas, mediante a utilização de procedimentos científicos. Nesta linha de pensamento, esta seção tem como propósito apresentar resumidamente a abordagem e procedimentos utilizados neste estudo, e as razões que justificam a escolha de cada um deles. Para realização da pesquisa foi utilizada a combinação de métodos e técnicas conforme sintetizado na Tabela 5.

Tabela 5 – Quadro Metodológico da Pesquisa

Quadro Metodológico	
Finalidade	Pesquisa aplicada
Natureza	Pesquisa descritiva
Forma de abordagem	Pesquisa quanti-qualitativa
Objetivos	Pesquisa exploratória
Estratégia	Estudo de caso
Método científico	Indutivo
Procedimentos técnicos	Pesquisa documental, bibliográfica e estudo de caso
Procedimentos para coleta de dados	Entrevistas, questionários e grupo focal

A tabela 5 apresenta de forma resumida o enquadramento metodológico deste trabalho. O estudo investiga a ineficiência em gerir riscos em aquisições de TIC no âmbito das instituições públicas brasileiras. A pesquisa tem o objetivo de levantar

informações de forma profunda e detalhada sobre gestão de riscos de forma a propor melhorias para o processo de aquisições de TIC.

Quanto à finalidade o estudo pode ser classificado como pesquisa de natureza aplicada. Segundo Kauark (2010) e Gil (2019) a pesquisa aplicada objetiva gerar conhecimentos para aplicação prática, dirigida à solução de problemas específicos.

Este estudo visa buscar conhecimento da área de gestão de riscos, a fim de gerar conhecimento que possa ser utilizado como um norteador para o entendimento da situação atual da Administração Pública Federal e com isso, propor melhorias para o gerenciamento de riscos em aquisições de TIC. Neste sentido, a natureza da pesquisa é descritiva, ou seja, realiza-se o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador (BARROS; LEHFELD, 2007).

Esta pesquisa traz novas discussões sobre aquisições de TIC no âmbito das instituições públicas brasileiras, a partir da realidade diagnosticada, juntamente com a adoção de técnicas, ferramentas e das boas práticas pesquisadas e amplamente utilizadas. Em geral, a forma de abordagem dos dados é quanti-qualitativa.

A pesquisa quantitativa é baseada no emprego da quantificação na coleta dos dados e no tratamento deles, por meio do tratamento estatístico. Já a abordagem qualitativa segundo Marconi e Lakatos (2017) é uma forma de analisar, interpretar e fornecer análise mais detalhada sobre as investigações, com o objetivo de prover informações exploratórias. A abordagem do problema é qualitativa, no qual se busca entender um fenômeno específico em profundidade, trabalha com descrições, comparações e interpretações ao invés de estatísticas, regras e outras generalizações (MARCONI; LAKATOS, 2017).

Em relação aos procedimentos técnicos, ou seja, a maneira de obtenção dos dados necessários para a elaboração do estudo, foram utilizadas pesquisa documental, bibliográfica e estudo de caso.

Quanto aos meios, a pesquisa é classificada como documental, visto que os materiais utilizados não tiveram tratamento analítico. Ela foi realizada em sites de órgãos de controle e institutos federais de educação que participaram deste estudo de caso. Ao realizar a pesquisa documental foram observados os documentos: PDI, PDTI, Relatórios de Gestão, Mapas de Riscos, Políticas de Gestão de Risco, Metodologia de Gestão de Risco e páginas sobre Licitações e Contratos.

Ainda com relação aos procedimentos, enquadra-se como pesquisa bibliográfica, uma vez que foram pesquisados os assuntos: aquisições de TIC, conceitos sobre riscos e gestão de riscos, abordagens e metodologias sobre gestão de riscos, sistematização em gestão de riscos e legislação vigente sobre a temática. A revisão bibliográfica foi feita a partir de bases de dados, em artigos científicos, livros, normas, dissertações e teses conforme apresenta as referências bibliográficas descritas neste documento.

O estudo de caso foi utilizado como estratégia de pesquisa pois aborda a questão “como”, e a pesquisadora teve pouco controle sobre os eventos e o foco foi direcionado para um fenômeno contemporâneo inserido no contexto da vida real das instituições públicas brasileiras (YIN, 2015).

A pesquisa envolveu um único caso buscando com isso reunir informações específicas por meio de estudo exaustivo de alguns objetivos, o que permitiu um conhecimento amplo e detalhado dos problemas relacionados, e uma possível solução (BOAVENTURA, 2011). Neste estudo foram realizadas entrevistas com pessoas com experiência prática em relação ao problema pesquisado. Além disso, foram aplicados questionários visando explorar mais sobre o conhecimento escondido (BOAVENTURA, 2011).

A coleta de dados seguiu as recomendações de Gil (2019) e Yin (2015) e foi feita através de entrevistas, grupo focal e questionários. Gil (2019) cita que os resultados obtidos no estudo de caso devem ser provenientes da convergência ou da divergência das observações de diferentes procedimentos, assim torna-se possível conferir a validade ao estudo.

Após a coleta de dados foi realizada uma análise das relações entre as variáveis para uma posterior determinação dos efeitos resultantes em instituições públicas brasileiras. O estudo classifica-se como exploratório porque as especificidades do ambiente são características únicas, que não foram exaustivamente discutidas ou encontradas na APF.

Portanto, a elaboração da solução proposta foi baseada em uma abordagem indutiva, ou seja, partindo de um conjunto de dados particulares, devidamente constatados, inferiu-se conclusões prováveis. A pesquisa considerou que o conhecimento é fundamentado na experiência, não levou em conta princípios preestabelecidos (GIL, 2019; MARCONI; LAKATOS, 2017).

3.2 MÉTODO DE PESQUISA

Um método de pesquisa é definido como a sequência de passos necessários para demonstrar que o objetivo proposto foi atingido, sendo assim, ao executar as etapas descritas no método serão obtidos resultados, e esses deverão ser convincentes. A definição do método de pesquisa é fundamental, pois auxilia o pesquisador a realizar sua investigação no sentido de responder seu problema de pesquisa (MARCONI; LAKATOS, 2017).

A utilização de um método, quando seguido adequadamente contribui para assegurar a validade da investigação (MARCONI; LAKATOS, 2017). A próxima seção detalha o método de pesquisa adotado.

3.2.1 Design Science Research

O método de pesquisa escolhido para o desenvolvimento do estudo foi o *Design Science Research* (DSR). DSR é uma abordagem que além de produzir ciência sobre a realidade, objetiva projetar uma realidade diferente, modificada por artefatos projetados para resolver problemas em determinados contextos (PIMENTEL et al., 2017).

DSR é um método de pesquisa orientado à solução de problemas que segundo March (1995); March e Storey (2008); Myers e Venable (2014) busca a partir do entendimento de uma situação real, construir e avaliar artefatos que permitam transformar a realidade, alterando suas condições para resultados melhores ou desejáveis (DRESCH et al., 2015). Para Dresch (2013) a solução do problema proposta por este método não necessariamente busca a solução ótima, mas sim, a solução satisfatória para a situação.

Neste sentido, a pesquisa tem como requisitos: ser constituída por fases distintas e sequenciais; ser iterativa, permitindo que, após as etapas de desenvolvimento e validação, sejam retornadas às etapas anteriores, caso necessário; ter etapas de avaliação e validação do artefato criado e deve apresentar os resultados obtidos com o uso da solução. Para que estes requisitos sejam atendidos optou-se por utilizar as etapas definidas na *Design Science Research*

Methodology proposta por Peffers et al. (2007), por ser uma metodologia que já foi utilizada por diversas publicações científicas, o que demonstra sua importância e relevância.

A metodologia DSR definida por Peffers et al. (2007) possui uma sequência lógica de etapas a serem seguidas podendo ser repetida de forma a melhorar a solução proposta. A figura 15 descreve as 6 etapas utilizadas para o desenvolvimento deste estudo.

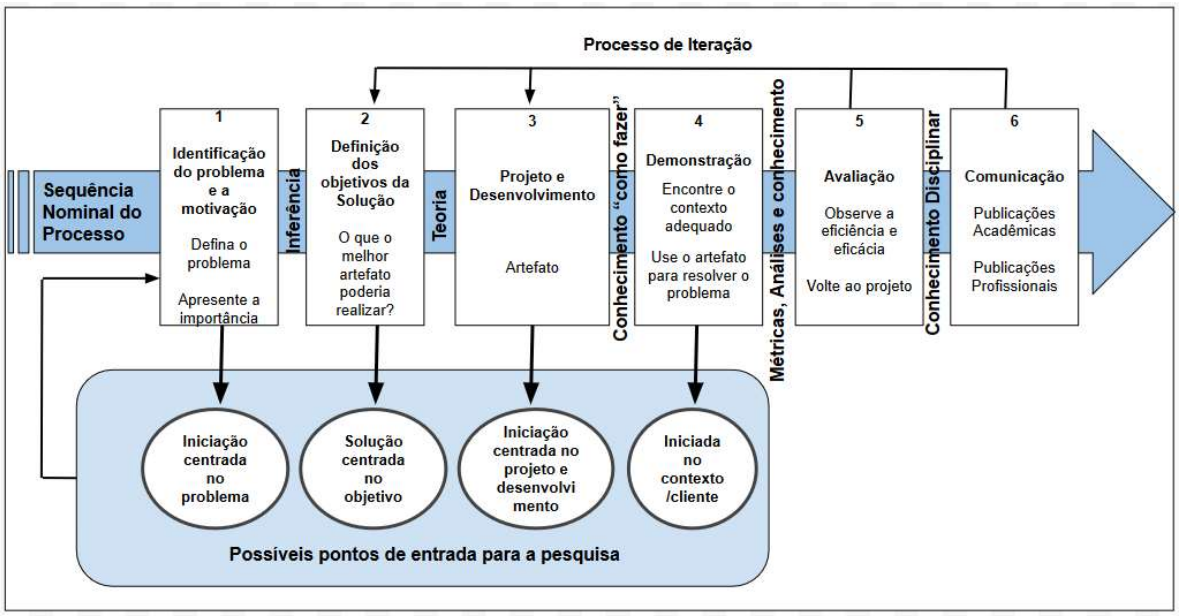


Figura 15 - Etapas da Pesquisa

Conforme apresenta a figura 15, a pesquisa iniciou com a revisão bibliográfica na etapa 1 feita através de artigos científicos, dissertações, teses, guias, metodologias, modelos e normas técnicas e legislações de forma a validar o problema a ser investigado, sua importância e a definição do tema da pesquisa. Em seguida, foram definidos os objetivos da solução proposta. Com isso, o projeto foi desenvolvido, demonstrado e avaliado. Por fim, os resultados são comunicados neste documento.

1 Identificação do Problema e a Motivação

Segundo Peffers et al. (2007), a etapa 1 da pesquisa inicia quando o pesquisador toma consciência do problema e justifica a sua importância, considerando sua

relevância para a sociedade. Ela busca compreender o problema antes de definir a solução. Esta etapa está descrita no capítulo 4.

No capítulo 4 o problema *ineficiência em gerir riscos em aquisições de TIC* é descrito a partir da análise de um conjunto de conceitos, teorias e relações verificadas, que foram úteis para explicar o processo utilizado na pesquisa para analisar os problemas relatados no levantamento de governança pública divulgados pelos TCU (TCU, 2017; 2018) e na literatura científica. Para apresentar o problema deste estudo foram aplicados dois questionários e realizadas entrevistas com servidores das áreas de Tecnologia da Informação e Administração, especialistas em aquisições de TIC.

Para a realização da pesquisa foram adotadas as providências necessárias, tais como: delimitação do escopo da pesquisa, elaboração e disponibilização dos questionários on-line, envio de convite para os respondentes por e-mail. Além dos procedimentos citados, foram feitos convites para a realização de entrevistas de forma a validar as informações obtidas através dos questionários.

A aplicação dos instrumentos de coleta de dados serviu para confirmação das causas para as dificuldades em gerir riscos no processo de aquisição, suas consequências, variáveis que influenciam a gestão de riscos, os controles utilizados e as possíveis soluções para o problema. Dessa forma, foi possível identificar a relevância da pesquisa para as instituições públicas brasileiras bem como a motivação para o estudo.

2 Definição dos Objetivos da Solução

Segundo Peffers et al. (2007) e Dresch (2013) a etapa 2 diz respeito à definição dos resultados esperados para o problema que está se buscando resolver, *ineficiência em gerir riscos no processo de aquisição de TIC*. Os objetivos da solução proposta neste estudo são:

- Estruturação e documentação das fases que envolvem a gestão de riscos em aquisições de TIC;

- Identificação de riscos e definição de controles de forma sistematizada sem depender da experiência do analista especialista em gestão de riscos;
- Transparência da gestão de riscos no processo de aquisição de TIC por meio de relatórios e gráficos sumarizados;
- Disponibilização de informações sobre riscos envolvendo o processo de aquisição de TIC através de uma planilha documentadora disponibilizada em um repositório digital de informações;
- Monitoramento e controle de todas as fases do processo de aquisição de TIC por meio de *checklists* e indicadores de desempenho.

3 Projeto e Desenvolvimento

Para Peffers et al. (2007), Vaishnavi e Kuechler (2005), o artefato é desenvolvido e implementado nesta etapa, visando auxiliar na resolução do problema que está sendo estudado. Para isso, o pesquisador deverá fazer uso do conhecimento teórico existente (capítulo 2), a fim de propor artefatos (capítulo 5) que suportem a solução do problema (PEFFERS et al., 2007).

Segundo Wieringa (2014), a solução pode ser proposta através de descrição em linguagem natural, diagramas, modelos matemáticos, protótipos ou pela combinação destes. Neste caso, optou-se por desenvolver uma metodologia contendo artefatos para o gerenciamento de riscos eficiente em aquisições de TIC, detalhada no capítulo 5, a partir de sugestões de melhorias feitas pelos participantes da investigação do problema, descrita no capítulo 4.

Para desenvolver a solução do problema apresentado neste estudo foram usados conceitos de modelos, normas e metodologias que são referências no mercado sobre gestão de riscos. Dentre as diversas referências existentes foram utilizadas as atividades previstas na norma ISO 31000 (2018), técnicas de avaliação de riscos apresentadas da norma ISO 31010 (2019), os guias de boas práticas em contratações de soluções de TI TCU (2012) e MPOG (2017) e os modelos COBIT (2013; 2019), e COSO ERM (2007, 2017), PMI (2017) e *The Orange Book* (HMG, 2019).

Também foram pesquisadas leis, guias, manuais, roteiros, artigos científicos, dissertações, teses e sites especializados sobre a temática. O referencial teórico utilizado na pesquisa encontra-se disponível nas referências bibliográficas. A etapa 3 está descrita no capítulo 5.

A solução construída nesta etapa contempla o desenvolvimento de dois artefatos: uma planilha documentadora contendo o inventário de riscos e controles para nortear a gestão de riscos em aquisições de TIC, e um repositório digital de informações para registro de lições aprendidas sobre gerenciamento de riscos.

Dentro da planilha documentadora (mapa de gerenciamento de riscos) foram configurados mapas, gráficos, planilhas e relatórios para documentar todas as etapas que compõe a solução. Para divulgar a solução desenvolvida de forma que outras instituições públicas possam utilizar, foi desenvolvido o repositório digital de informações GRATIC que contém detalhes sobre a metodologia, os artefatos construídos, bem como os materiais de referência utilizados. O endereço eletrônico do repositório digital de informações está disponível no apêndice H.

4 Demonstração

A etapa 4 consiste no uso da solução de forma prática no contexto investigado (WIERINGA, 2014). Esta etapa refere-se ao uso do artefato para solucionar o problema em questão, podendo ser efetuada por meio de experimentação, simulação, estudo de caso, pesquisa-ação (DRESCH, 2013). Neste caso, optou-se pelo estudo de caso, descrito no capítulo 6.

O contexto para a realização do estudo de caso foi o cenário das instituições públicas brasileiras. Nesta etapa foi escolhido um Instituto Federal de Educação da região norte do país, tendo em vista a facilidade de acesso aos participantes da equipe de planejamento de aquisições e informações sobre os processos de aquisições em andamento. Esta etapa está descrita no capítulo 6.

Para demonstrar que o uso da solução proposta é viável para as demais instituições públicas brasileiras, foram escolhidos dois processos licitatórios de aquisições de TIC que são comuns a todas as entidades que fazem parte da Administração Pública Federal. São eles: aquisição de equipamentos de informática

e contratação de empresa especializada em prestação de serviços de link de internet.

5 Avaliação

Segundo Peffers et al. (2007), Vaishnavi e Kuechler (2005) e Manson (2006), a etapa 5 explica o que deve ser analisado e testado de acordo com as condições estabelecidas para validação. A etapa de avaliação contribuiu para o processo de melhoria do artefato construído. A etapa 5 está detalhada no capítulo 6.

O pesquisador deverá observar e medir como o artefato se comporta no sentido de solucionar o problema que está sendo estudado (Peffers et al., 2007 e Dresch, 2013), com o que havia sido definido como requisitos para a solução do problema. Caso o resultado encontrado não seja o esperado, o pesquisador poderá retornar à etapa de Projeto e Desenvolvimento, a fim de desenvolver um novo artefato (PEFFERS et al., 2007).

No caso deste estudo a solução proposta foi avaliada pelos membros da atual equipe de planejamento da contratação do Instituto Federal de Educação escolhido para realização do estudo de caso. A etapa de avaliação considerou a capacidade de executar a tarefa pretendida ou a capacidade das pessoas utilizarem a solução proposta, observando eficiência, generalidade e facilidade de uso, conforme recomenda DRESCH (2013).

6 Comunicação

A etapa 6 consiste em comunicar tanto o problema que foi estudado como, também, sua importância e como ele pode ser solucionado. Ademais, é nessa etapa que deverá ser apresentado o rigor com o qual a pesquisa foi conduzida, bem como o quão eficaz foi a solução encontrada para o problema (DRESCH, 2013).

Segundo Manson (2006), Vaishnavi e Kuechler (2005) e Peffers (2007), isso significa que o pesquisador aprende algo novo e, caso as coisas não funcionem de acordo com a teoria, o pesquisador deve analisar o que está acontecendo, e por que isso sucedeu. Caso o resultado não for o esperado deve-se retornar a etapa de

identificação do problema, quando novos conhecimentos podem ser adquiridos para que se refinam os limites da incompleta teoria que foi usada para criar o artefato.

O resultado da etapa 6 está descrito no capítulo 7. Como forma de explicitar como a pesquisa foi desenvolvida a tabela 6 apresenta as etapas com seus respectivos pontos a serem explicitados e as saídas.

Tabela 6 - Pontos a Explicitar na Condução da Pesquisa

Etapa da Pesquisa	Ponto a explicitar	Saída
Identificação do problema e motivação	- Evidenciar a situação problemática e justificar o valor (importância) de uma solução. - Apresentar o estado da arte relacionado à temática da pesquisa.	Capítulo 1, 2 e 4
Definição de objetivos da solução	- Explicitar as premissas e requisitos para a construção dos artefatos para solução do problema.	Capítulo 1 e 3
Projeto e desenvolvimento	- Justificar a escolha das ferramentas para o desenvolvimento do artefato. - Determinar a funcionalidade do artefato e sua arquitetura. - Definir e criar artefatos.	Capítulo 5
Demonstração e Avaliação	- Os artefatos deverão ser colocados à prova. - Detalhar os mecanismos de avaliação do artefato. - Explicitar as partes envolvidas. - Evidenciar o que funcionou como o previsto e os ajustes necessários.	Capítulo 6
Comunicação	- Comunicar o problema e sua importância, o artefato e sua utilidade. - Sintetizar as principais aprendizagens em todas as fases do projeto. - Justificar a contribuição do trabalho para a classe de problemas em questão.	Capítulo 7

A tabela 6 apresenta os pontos a serem detalhados em cada uma das etapas da pesquisa e as saídas associadas, a partir de Manson (2006), Peffers et al. (2007) e Lacerda (2013). Nesta tabela, procurou-se indicar os mecanismos que possibilitam a compreensão detalhada dos capítulos produzidos e, por consequência, garantam a replicação deste estudo.

3.3 MÉTODO DE INVESTIGAÇÃO

Para investigar, solucionar, avaliar e propor a solução foi utilizado o estudo de caso. Segundo Yin (2015) um estudo de caso é uma pesquisa considerada empírica que busca melhor compreender um fenômeno contemporâneo, normalmente complexo no seu contexto real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos.

Siau e Rossi (2007) relatam que estudos de caso não exigem que os pesquisadores intervenham nas operações normais das organizações e as instituições geralmente aceitam que a pesquisa seja conduzida. Para Yin (2015) a principal vantagem do uso de estudo de caso é a riqueza de dados, algo que as pesquisas e experiências são incapazes de combinar.

Yin (2015) afirma que o estudo de caso pode ser aplicado quando uma pergunta “como” (exploratória) está sendo feita sobre um conjunto contemporâneo de eventos nos quais o pesquisador tem pouco ou nenhum controle. Estudo de caso descreve fenômeno, ajuda os pesquisadores a construir teorias ou testar conceitos e relacionamentos teóricos existentes.

O estudo caso foi único e estudou um contexto real (ineficiência em gerir riscos em aquisições de TIC no âmbito das Instituições Públicas Brasileiras). As etapas do estudo de caso seguiram o método de pesquisa DSR proposto por Peffers et al. (2007).

O protocolo adotado para o estudo de caso foi construído conforme recomenda Yin (2015), ou seja, uma visão geral do projeto de estudo de caso, os procedimentos a serem adotados no campo, questões de estudo de caso utilizadas nas entrevistas, um guia para o relatório de estudo de caso. Os apêndices E e G apresentam artefatos criados especificamente para o estudo de caso.

A estratégia da pesquisa utilizou um Instituto Federal de Educação como um caso a ser estudado, com a coleta dos dados sobre a gestão de riscos no processo de aquisições de TI no contexto real. Para complementar o estudo foram realizadas pesquisas documentais em materiais que não receberam tratamento analítico, como documentos, normas, políticas, relatórios e manuais de forma a validar as conclusões obtidas.

A análise do trabalho é baseada em um estudo de caso que generaliza as percepções e avaliações. Em razão da complexidade do estudo de riscos e, principalmente, a respeito de contratação de TIC ser ampla, a pesquisa serve de ponto de partida para a implantação ou atualização de uma metodologia prática para a gestão de riscos em contratações de TIC nas instituições públicas brasileiras.

O estudo de caso em tela foi constituído a partir de uma combinação de métodos de coleta de dados, como entrevistas, questionários, observações. Estas evidências serviram de subsídio para fundamentar a metodologia proposta. A próxima seção detalha os métodos e técnicas de coleta de dados utilizados neste estudo.

3.4 MÉTODOS E TÉCNICAS DE COLETA DE DADOS

A coleta de dados para validar a investigação do problema foi feita por meio de entrevistas, que é uma das fontes de informações utilizadas para a realização da pesquisa. Segundo Severiano (2010) as entrevistas permitem ao sujeito uma interação e pode fazer argumentação para o pesquisador compreender o pensamento do entrevistado.

Para Yin (2015), as entrevistas constituem uma fonte de dados essencial e na maioria das vezes aborda questões humanas, além de também fornecer inferências causais percebidas. As entrevistas com especialistas na área de aquisições de TIC possibilitaram a investigação dos motivos pelos quais as instituições têm dificuldades de realizar a gestão de riscos, quais são os problemas mais recorrentes e os fatores críticos de sucesso para a melhoria do processo de contratação de soluções de TIC.

A validação da investigação foi realizada de forma documental permitindo o que foi dito, ou escrito a respeito de determinado assunto, pudesse ser estudado sob um novo enfoque o que possibilitou inclusive novas descobertas sobre o assunto (MARCONI, 2017). A revisão bibliográfica através de busca por materiais como livros, dissertações e artigos com reconhecimento científico possibilitou descobrir as publicações sobre a temática a ser estudada (GIL, 2019).

Os questionários foram utilizados de forma a investigar o problema em seu contexto real. Além disso, foram utilizados para avaliar a solução proposta no estudo. Uma série de perguntas foram feitas aos entrevistados com o intuito de

compreender a visão dos especialistas na área de aquisições de TI. Os questionários foram respondidos por escrito e sem a presença da pesquisadora conforme sugere Marconi e Lakatos (2017).

3.5 MÉTODO DE ANÁLISE E SÍNTESE DE DADOS

O procedimento de análise de dados de acordo com Yin (2015) consiste em examinar, categorizar, classificar em tabelas ou, do contrário, recombinar as evidências tendo em vista proposições iniciais de um estudo. Nesta pesquisa foram utilizadas categorias para análise dos resultados das entrevistas para melhor compreensão dos dados.

Para analisar e apresentar os dados, foi selecionada também a abordagem de análise temática apresentada por Cruzes e Dyba (2011). Estes autores destacam que a análise temática é uma abordagem frequentemente utilizada para identificar padrões em uma análise qualitativa.

Segundo Marconi e Lakatos (2017) a análise temática permite maior compreensão do texto, fazendo emergir a ideia central e as secundárias, as unidades e subunidades de pensamento, sua correlação e a forma como ocorre. A análise ou síntese temática identificou temas recorrentes da coleta de dados e organizou as informações em temas específicos.

Neste propósito os dados foram categorizados por assuntos relacionados a temática da pesquisa. Em seguida, foram avaliados por especialistas na área de contratações de TIC do instituto federal de educação, utilizado como estudo de caso, por meio de grupo focal e entrevistas o que possibilitou a correlação das informações.

3.6 REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica consistiu em realizar uma análise aprofundada no acervo de publicações existentes na área pesquisada, com a finalidade de buscar respostas ou um maior conhecimento sobre gestão de riscos no processo de aquisição de TIC. Para realizar esta atividade foram utilizadas bases de dados e adotados os critérios de análise que serão abordados nas próximas seções.

3.6.1 Bases de Dados

As bases de dados utilizadas para consulta foram: *Google Scholar* e *CAPES (IEEE Xplorer, ACM Digital Library, Scopus, Springer Link, Web of Science* e *Science Direct*). Vale ressaltar que cada base de dados possui características e limitações próprias e que os motores de busca trabalham de maneira diferente. Assim, a *string* de busca foi adaptada para rodar adequadamente em cada base (WHOLIN et al., 2013).

No momento da realização das buscas foi observada se a base considerava termos no plural ou se os mesmos deveriam ser adicionados à *string*, se a base permite realizar buscas considerando apenas partes do texto (título, resumo e palavra-chave) ou se as pesquisas são feitas sempre levando em consideração o texto completo. A base IEEE Xplorer por exemplo impõe limitação quanto ao número de caracteres ou de termos, fato que fez com que a *string* de busca fosse dividida em partes menores o que demandou múltiplas consultas e a retirada dos estudos duplicados em cada consulta realizada.

3.6.2 Critérios de Análise dos Trabalhos Científicos e Técnicos

Os critérios para a análise dos trabalhos científicos e técnicos foram divididos em critérios de inclusão e exclusão:

a) Critérios de inclusão

- Estudos primários ou secundários que abordem gestão de riscos em contextos governamentais.
- Estudos publicados entre os anos de 2014 e 2019.
- Trabalho analisado se baseia em alguma abordagem que é referência em gestão de riscos?
- Quais atividades, ferramentas e técnicas são utilizadas pelos trabalhos analisados?
- Proposta analisada teve alguma aplicação prática?

b) Critérios de exclusão

- O artigo não tem um resumo (abstract).
- Trabalhos que não foram escritos em inglês ou português.
- Trabalhos que utilizem *gestão de riscos* para outros fins que não predominantemente no contexto de governança pública ou que apenas façam menção ao tema.
- Estudos que utilizem o termo "*management risk*" com significados não relacionados à definição explicitada para o setor público.
- Estudos duplicados/redundantes de mesma autoria.
- Estudos que não foram publicados entre os anos de 2014 e 2019.
- Não foi possível ter acesso ao trabalho completo.

3.6.3 Procedimentos de Busca

A seleção dos trabalhos relacionados foi fundamental neste estudo, pois foi a base teórica para a proposta de metodologia de gestão de riscos voltada para aquisições de TIC. Através da pesquisa bibliográfica foram obtidas as perspectivas necessárias para proposta da metodologia GRATIC.

Para definir a *string* de busca foram adotadas várias abordagens, tais como Petersen et al. (2015) relata: consultar especialistas, melhorar iterativamente a *string,* identificar termos a partir de artigos conhecidos. O procedimento de busca genérico adotado pelo estudo utilizou palavras chaves, *strings*: *("risk management") AND (("risk of methodology" OR "enterprise risk management" OR "risk management government") AND ("risk management" OR "methodology information technology" OR "methodological principles risk management")).* Esta *string* de busca foi adaptada de acordo com as particularidades de cada base de dados, por exemplo foram substituídos os operadores lógicos (OR) e (AND) pelos operadores <or> e <and>.

Para a definição da *string* de busca, definiu-se como foco a identificação de termos relacionados à temática da pesquisa que sejam utilizados com frequência nos estudos primários. Adotou-se a prática de formular a *string* por meio de agrupamento de termos relativos ao mesmo aspecto, ou seja sinônimo.

4 INVESTIGAÇÃO DO PROBLEMA

O capítulo aborda como as instituições públicas brasileiras realizam a gestão de riscos no processo de aquisição de TIC. Inicia apresentando a situação atual das instituições públicas em relação a gestão de riscos. Em seguida, descreve o estado atual da gestão de riscos em aquisições de TI no contexto dos Institutos Federais de Educação. Depois apresenta as causas para a dificuldade em gerir riscos em aquisições de TIC. Por fim, detalha os requisitos para a solução do problema, segundo a opinião dos participantes dos questionários 1 e 2 e entrevistas realizadas.

4.1 SITUAÇÃO ATUAL DAS INSTITUIÇÕES PÚBLICAS BRASILEIRAS

O Tribunal de Contas da União (TCU) vem realizando auditorias nos últimos anos para conhecer a situação atual das organizações públicas em relação a governança e gestão com a finalidade de estimular as entidades públicas a adotarem boas práticas e melhorarem seus níveis de maturidade e tentar resolver o problema da ineficiência em gerir riscos em aquisições de TIC. Em 2018, publicou o Acórdão Nº 2699/2018 que apresenta o levantamento realizado com 498 instituições da Administração Pública Federal.

Este levantamento mede a capacidade de governança e gestão das organizações públicas federais e de outros entes jurisdicionados do TCU, ao aferir o nível de implementação de boas práticas de liderança, estratégia e *accountability*, bem como de práticas de governança e gestão de TI, de pessoas e de contratações. Neste levantamento é possível observar que em organizações que não há governança de contratações, há maior exposição a riscos, desperdício de recursos públicos e irregularidades nas aquisições (TCU, 2018d).

Dentro do cenário de governança pública brasileiro, percebe-se que a deficiência em gerir riscos, não abrange apenas a área de gestão de contratações, mas a organização como um todo (TCU, 2018d). Conforme pode ser verificado na figura 13, a maioria das instituições públicas estão no nível inicial ou inexpressivo de gestão de riscos. Possivelmente, este índice expressivo se deve a inexistência de procedimentos padronizados para realizar a gestão de riscos, falta de

planejamento da contratação, inexistência de sistematização de rotinas de trabalho e deficiência na comunicação entre setores.

A partir das informações apresentadas no relatório técnico completo de acompanhamento de governança pública publicado pelo TCU em 2018 (TCU, 2018f) é possível verificar que o percentual do agregador riscos em contratações é bastante expressivo, conforme apresenta a figura 16. Ao analisar as informações divulgadas no levantamento de governança pública (ciclo 2018) é possível perceber uma evolução na gestão de riscos se comparado aos outros anos, mas há muito o que ser feito pela maioria das entidades públicas, uma vez que 81% das organizações estão no estágio inicial e inexpressivo em relação a gerir os riscos críticos da organização como um todo (TCU, 2018f).

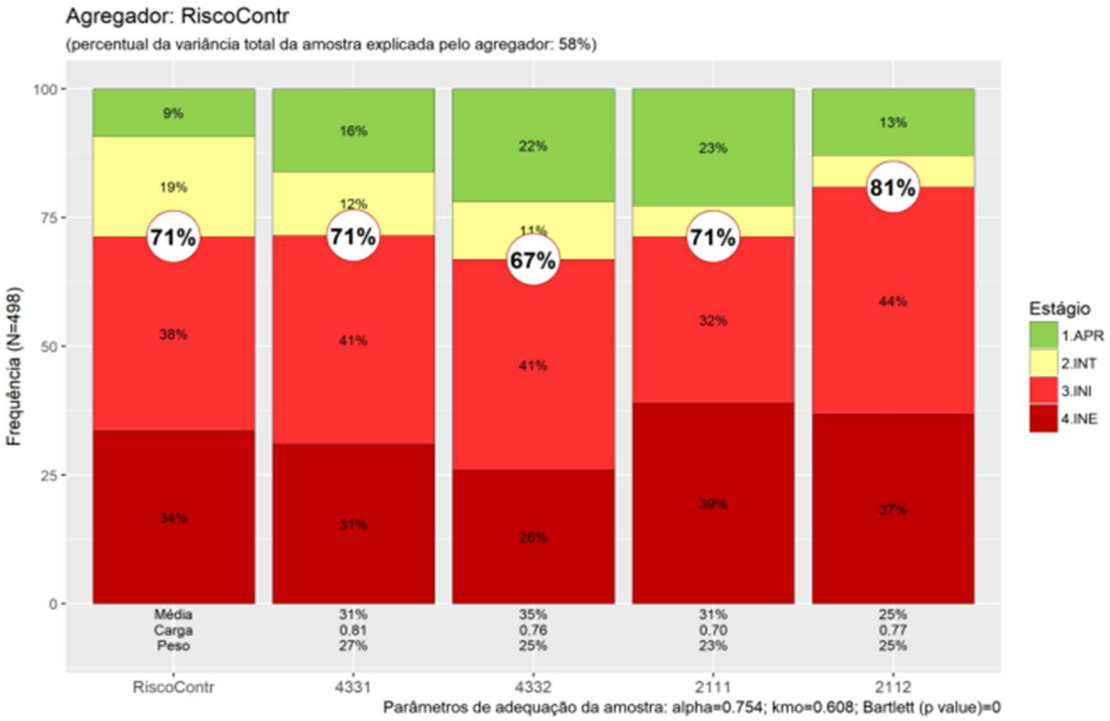


Figura 16 - Riscos em Contratações

Os dados apresentados na figura 16 são preocupantes, pois revelam a baixa maturidade em gestão de riscos em contratações públicas. Para 71% dos participantes que responderam o levantamento sobre governança pública (ciclo 2018), o estágio é inexistente ou inexpressivo em relação ao estabelecimento do modelo de gestão de riscos. Pode-se afirmar que a ausência da função gestão de

riscos está correlacionada com o quadro deficiente apresentado na gestão de contratações (TCU, 2018d).

Em relação à gestão de riscos na área de contratações, 71% afirmam ser inexistente ou inexpressivo. Cerca de 67% das instituições que participaram do levantamento de governança pública afirmam que estão em estágio inexistente e inexpressivo em relação à análise de riscos que possam comprometer a efetividade das etapas de planejamento da contratação, seleção do fornecedor e gestão contratual ou que impeçam ou dificultem o atendimento da necessidade que originou a contratação (TCU, 2018d).

Embora algumas instituições possuam planos, políticas, normativas, metodologias sobre a gestão de riscos de forma geral abrangendo toda a organização, não foi possível identificar, através de pesquisa documental utilizando os relatórios de gestão, PDTI e site institucional, como estas instituições públicas realizam a gestão de riscos no processo de aquisição de TIC. Este ponto é importante e requer atenção, uma vez que põe em cheque o alcance dos objetivos da organização ou de cada subárea (contratações, TI, pessoas). Por isso, optou-se por realizar a investigação do problema, através de questionários semiestruturados apresentados nos apêndices C e D.

4.2 ESTADO ATUAL DA GESTÃO DE RISCOS EM AQUISIÇÕES DE TIC

A gestão de riscos no contexto das instituições públicas brasileiras é um dos grandes desafios enfrentados nos últimos anos (TCU, 2017; 2018d). No processo de aquisição de TIC, envolve estabelecimento do contexto, identificação, avaliação, tratamento, monitoramento e comunicação de eventos que possam afetar o cumprimento dos objetivos organizacionais. Neste sentido, o TCU considera como urgente a adoção de medidas que visem implementá-la e aperfeiçoá-la nos diversos órgãos e entidades da APF (TCU, 2018d).

Através de pesquisas realizadas em sites dos Institutos Federais de Educação foi possível verificar que são divulgadas informações apenas sobre a identificação e planos de tratamento de riscos em aquisições de TIC. Segundo os participantes do questionário 2, grande parte das instituições utilizam o site de compras governamentais, o sistema eletrônico de informações (SEI) e o sistema

unificado de administração pública para publicar atos administrativos sobre aquisições de TIC e monitorar e controlar riscos. Porém as informações não estão disponíveis de forma transparente para a sociedade.

Os participantes do estudo relatam que a maioria das informações sobre a gestão de riscos em aquisições de TIC não estão visíveis para todos, como por exemplo como é realizado o monitoramento, controle, registro e relato de riscos no decorrer da execução das fases do processo aquisitivo, uma vez que a legislação não torna obrigatória a divulgação de todos os artefatos deste processo. Neste sentido, os documentos gerados são compartilhados e acessados apenas por membros da equipe de planejamento da contratação da organização.

De forma a compreender como a gestão de riscos é realizada na prática no processo de aquisição de TIC foi adotada a estratégia de coleta de dados através de questionários e entrevistas com alguns Institutos Federais de Educação. Em seguida, para validar as informações apresentadas nos questionários 1 e 2 e solucionar dúvidas sobre o estado atual da gestão de riscos em aquisições de TIC foram realizadas entrevistas com especialistas na área de aquisições de TIC do Instituto Federal de Educação que participou do estudo de caso.

4.2.1 Questionário 1: Processo de Aquisições de TIC

O primeiro questionário foi construído de forma a compreender como o processo de aquisição de TIC é executado nos Institutos Federais de Educação que compõem a APF. Este questionário foi composto por 18 questões, sendo 12 com respostas previamente definidas e 6 questões subjetivas. As questões visam identificar qual é a legislação utilizada, quais são os desafios enfrentados, quais são as boas práticas adotadas, se a instituição possui plano anual de contratações, quais são as causas para as dificuldades em gerir riscos, se o processo precisa ser melhorado e quais as sugestões de melhoria.

O questionário 1, disponibilizado no apêndice C, foi aplicado no início do mês de junho de 2019 envolvendo 30 servidores públicos de 18 Institutos Federais de Educação, listados no apêndice A. O perfil dos participantes deste questionário encontra-se disponível no apêndice B. A média de participantes por Instituto Federal de Educação é dois servidores públicos por instituição.

Dentre as questões apresentadas no questionário 1, uma questão desperta atenção: quando os participantes foram questionados sobre o processo de aquisição de TIC em seu Instituto (questão 13), apenas 3,3% dos participantes avaliam como ótimo. Cerca de 6,7% avaliaram como bom, ou seja apenas 10% dos participantes consideram que o processo não precisa de melhorias, conforme apresenta a figura 17.

Apesar dos participantes que responderam o questionário 1 relatarem que existam guias e manuais sobre boas práticas em contratação de TIC é razoável concluir através de documentos disponibilizados nos portais institucionais, que cada instituição demora para adotar as recomendações existentes nas Instruções Normativas. Dados do questionário 1 (questão 5) mostram que apenas 20% dos Institutos Federais de Educação, participantes desta pesquisa adotam as recomendações da Instrução Normativa SGD/ME Nº 1, de 4 de abril de 2019, sobre contratações de TIC.

Sendo assim, cada instituição de ensino tem executado o processo de forma diferente, não seguindo o padrão estabelecido pelo governo federal, o que muitas das vezes acaba dificultando a execução do processo. A figura 17 apresenta o resultado sobre a avaliação do processo de aquisição de TIC nos Institutos Federais de Educação que participaram deste estudo (questão 13).

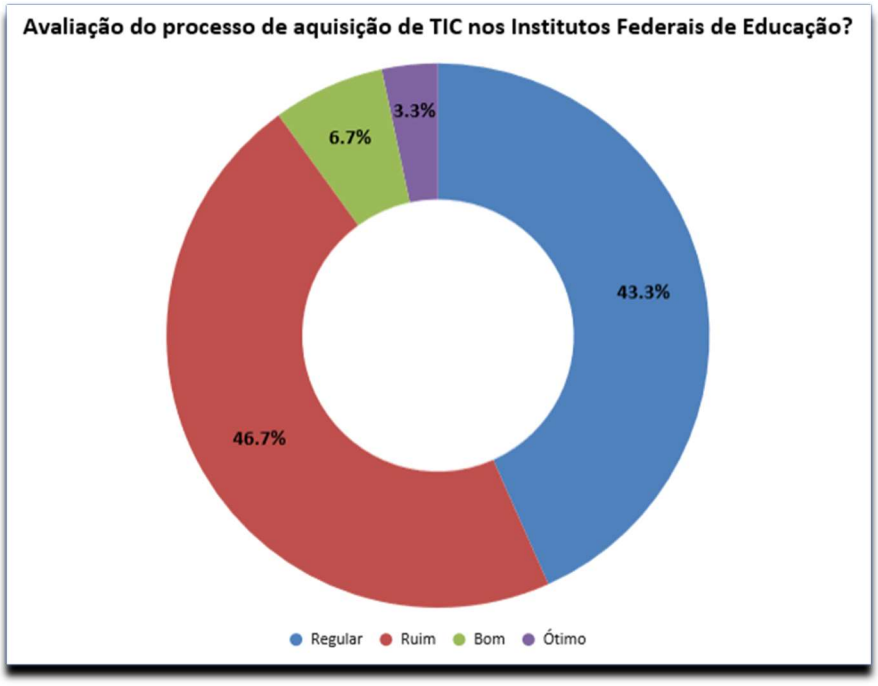


Figura 17 - Avaliação do Processo de Aquisições de TIC

Os dados apresentados na figura 17 mostram o cenário preocupante dos Institutos Federais de Educação que participaram da pesquisa. Para a maioria dos participantes do questionário 1, cerca de 90%, consideram que o processo de aquisição de TIC deve ser melhorado.

Segundo os participantes do questionário 1, na maioria das vezes, o processo não é conhecido por todos, é inflexível, lento, não é transparente e nem todos os atos administrativos são públicos. De acordo com 46,7% dos participantes deste estudo, sua instituição não divulga todos os artefatos gerados (questão 11) e 33,3% afirmam divulgar apenas alguns.

Estas informações demonstram que muitos Institutos Federais de Educação que participaram deste estudo não adotam as recomendações da legislação vigente, o que apresenta coerência com os dados divulgados pelo TCU, no relatório técnico de auto avaliação realizado pelas instituições públicas (TCU, 2018g). O apêndice A mostra o nível de gestão de riscos em contratações de cada instituição participante deste estudo.

Segundo relatos dos participantes desta investigação é possível afirmar que a gestão de riscos em aquisições de TIC tem muito a evoluir. A figura 18 apresenta o percentual de participantes que consideram necessária a realização de melhorias no processo (questão 14).

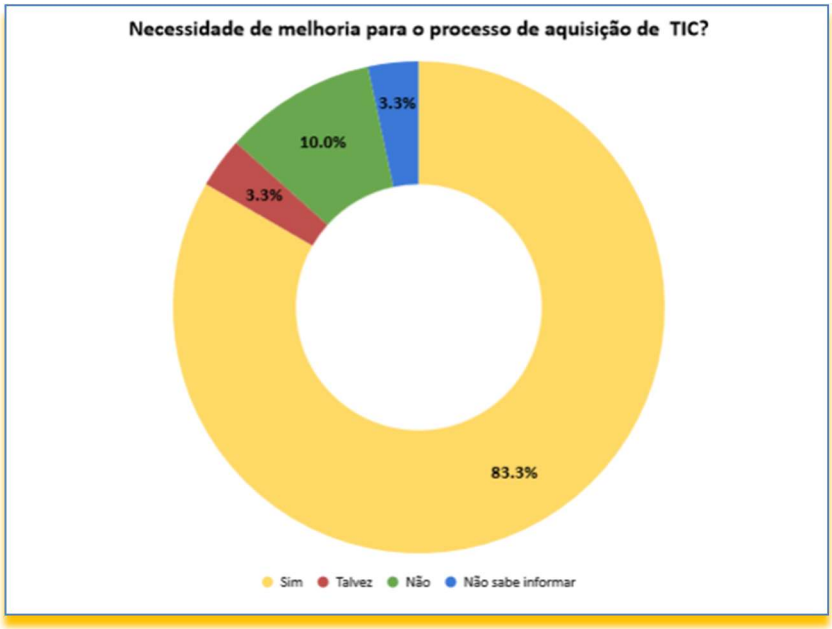


Figura 18 - Necessidade de Melhoria do Processo de Aquisições de TIC

A partir dos dados apresentados na figura 18 verifica-se que 83,3% dos participantes do questionário 1 (questão 14) consideram que o processo precisa ser melhorado e apenas 10% acreditam que não seja necessário, 3,3% não souberam informar e 3,3% Talvez. Os dados apresentados nesta figura demonstram que o processo de aquisições de TIC dos Institutos Federais de Educação, participantes deste estudo, possui fragilidades que devem ser corrigidas a fim de que evite o não cumprimento das metas estabelecidas nos objetivos organizacionais.

Para os participantes do questionário 1 que responderam a questão 17 as dificuldades encontradas no processo de aquisição de TIC podem ser minimizadas com a gestão de riscos efetiva nas fases que compõe o processo de aquisição. De acordo com um dos participantes, para que o processo seja melhorado é necessário "*definir fases para a gestão de riscos durante a execução de todo o processo*".

Já outro indica que a "*instituição deve encontrar indicadores que traduzam mais fielmente impactos de investimentos e ações tecnológicas; a instituição deve garantir uma plataforma de informações sobre as últimas aquisições e contratações; e garantir a feitura de relatórios de análise técnica anterior e posterior as contratações*". Por fim, outro participante recomenda que seja realizado o "*monitoramento contínuo de riscos e que sejam realizadas reuniões periódicas para acompanhamento e controle do processo de aquisição*".

Tendo em vista que 83,3% dos participantes do questionário 1 (questão 14), mencionam a necessidade de melhoria do processo a partir da definição de procedimentos operacionais padronizados para gestão de riscos em todas as fases do processo de aquisições de TIC, foi aplicado outro questionário visando compreender como a gestão de riscos é realizada na prática, quais são as dificuldades encontradas nos Institutos Federais de Educação e quais são as sugestões de melhoria. A próxima seção apresenta os resultados desse questionário.

4.2.2 Questionário 2: Gestão de Riscos em Aquisições de TIC

Conforme informações obtidas sobre a avaliação do processo de aquisições de TIC nos Institutos Federais de Educação que participaram do questionário 1, foi observado que o processo é complexo e requer melhorias em relação a gerir os riscos. Com a finalidade de compreender como é feita a gestão de riscos em aquisições de TIC, quais fases, técnicas, ferramentas e artefatos são utilizados pelos Institutos Federais de Educação, aplicou-se um segundo questionário no início do mês de julho de 2019, de forma a propor melhorias de acordo com o contexto atual das instituições públicas.

Este questionário foi respondido por 18 servidores públicos que participam atualmente da equipe de planejamento da contratação dos institutos federais de educação listados no apêndice A, ou seja, o estudo utilizou como público-alvo, as mesmas instituições que participaram do questionário 1, sendo que no questionário 2 foi respondido apenas por 1 participante de cada instituição. Os perfis dos participantes estão apresentados no apêndice B. O questionário é composto por 23 questões sendo que 17 são questões com respostas previamente definidas e 6 são discursivas. Este questionário está disponível no apêndice D.

As questões apresentadas no questionário 2 têm a finalidade de compreender e avaliar a gestão de riscos em aquisições de TIC nos Institutos Federais de Educação de forma a propor melhorias para o processo. Para isso, buscam entender como a instituição realiza a gestão de riscos em aquisições de TIC, qual é o processo de gestão de riscos adotado, quais são os problemas ocasionados pela falta da gestão de riscos, qual variável possui maior influência, quais são as técnicas, ferramentas, artefatos e procedimentos utilizados, o que deve conter o plano de tratamento de riscos, como é feito o monitoramento e controle de riscos, qual seria a solução ideal para gerir riscos em aquisições de TIC, como deve ser realizada a documentação e comunicação de riscos e lições aprendidas, quais são as dificuldades para gerir riscos no processo de aquisições de TIC.

Ao observar as respostas apresentadas na questão (4) pelos participantes do questionário 2, verifica-se que a maioria dos Institutos Federais de Educação participantes desta pesquisa utilizam diversas abordagens para realizar a gestão de

riscos: metodologias, planos, políticas, processos, normativas. Apenas 16,7% seguem a recomendação da Instrução Normativa SGD/ME Nº 1, de 4 de abril de 2019. A figura 19 apresenta os resultados obtidos na questão (4), "*Como sua instituição realiza a gestão de riscos no processo de aquisição de TIC?"*.

Figura 19 – Gestão de Riscos em Aquisições de TIC no Âmbito dos IFES

Conforme mostra a figura 19 observa-se que 33,3% dos participantes da pesquisa usam a política de gestão de riscos da própria instituição, 22,2% utilizam o plano de gestão de riscos definido pela instituição, 16,7% adotam as recomendações da Instrução Normativa SGD/ME Nº 1 de 4 de abril de 2019, 11,1% estabelecem uma metodologia própria de gestão de riscos, 11,1% usam a Instrução Normativa MPOG Nº 5 de 25 de maio de 2017 e 5,6% não realizam formalmente a gestão de riscos como prática sistemática.

Quando os participantes são questionados sobre o processo de gestão de riscos em aquisições de TIC, questão (7), conforme apresenta a figura 20, apenas 5,6% afirmaram que a gestão de riscos em aquisições é executada de forma satisfatória. Os demais participantes consideram que são necessárias melhorias.

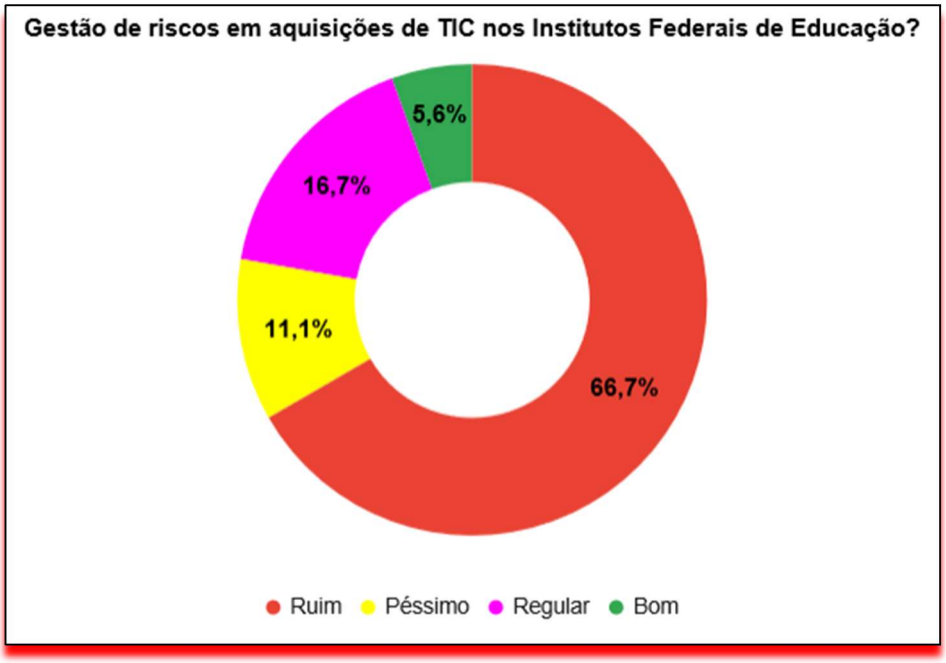


Figura 20 - Avaliação da Gestão de Riscos em Aquisições de TIC

A partir das informações apresentadas na figura 20 percebe-se que a maioria participantes do questionário 2, cerca de 66,7% consideram que a gestão de riscos no processo de aquisições de TIC em sua Instituição não é realizada de forma eficiente. Nenhum participante avaliou como “Ótimo”. Ao comparar as informações apresentadas no levantamento de governança pública divulgado pelo TCU em 2018, observa-se que são praticamente as mesmas percepções o que valida os dados coletados nesta investigação (TCU, 2018d).

Ao avaliar as informações apresentadas no questionário 2 (questão 22) é possível observar algumas semelhanças entre as dificuldades encontradas para uso de uma solução para gerir riscos em aquisições de TIC nos Institutos Federais, como por exemplo, 4 participantes afirmam que não existem capacitações específicas em gestão de riscos, 3 participantes relatam a inexistência de planejamento das atividades envolvendo o processo aquisitivo, 3 participantes afirmam que não são definidos procedimentos padronizados para realização das atividades de gestão de riscos, cerca de 5 participantes relatam a má comunicação envolvendo os setores e a falta de normativas internas sobre gestão de riscos.

Na visão dos participantes do questionário 2, a gestão de riscos em contratações de TIC é considerada como efetiva quando se tem o controle das variáveis que influenciam a melhoria do processo. Neste sentido, a figura 21

apresenta o percentual obtido em cada variável segundo a análise dos participantes que responderam a questão (9).

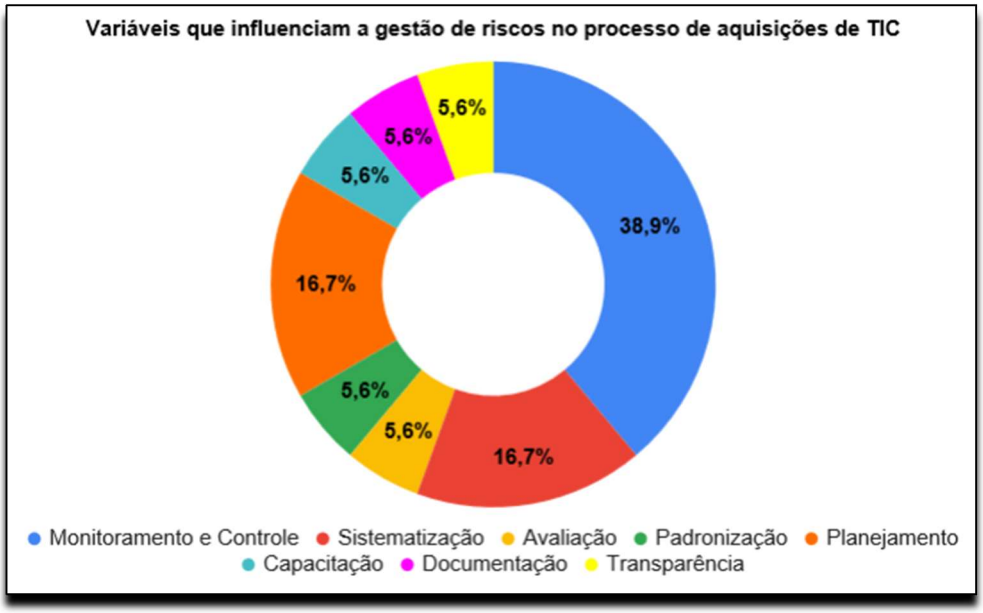


Figura 21 - Variáveis Influenciadoras para Gestão de Riscos em Aquisições

Conforme apresenta a figura 21, cerca de 38,9% dos participantes da pesquisa consideram o monitoramento e controle como sendo fundamentais para a eficiência da gestão de riscos no processo de aquisição de TIC. Para 16,7% dos participantes o planejamento da contratação e a sistematização das atividades são essenciais para que o processo seja realizado de forma eficiente. Em seguida, a padronização dos documentos, avaliação de riscos, a documentação das atividades, a capacitação dos servidores e a transparência dos atos administrativos aparecem com 5,6%.

Segundo relato de um dos participantes que responderam a questão (21) do questionário 2 sobre sugestão de melhoria “a instituição deve definir *fases para controle efetivo de riscos através da identificação de riscos em todas as fases da contratação; realizar a análise e avaliação de riscos a fim de definir as causas, probabilidade e consequências, sobre os objetivos organizacionais; tratar os riscos através de um plano de ação; monitorar e realizar análise crítica dos controles aplicados através de listas de verificação e registro e relato de lições aprendidas durante o processo licitatório podendo ser disponibilizadas através de um repositório digital de informações existente na organização*”. Outro participante sugere que “*a gestão de riscos deve monitorar e controlar riscos do processo de*

aquisições de TIC do início ao fim, conforme recomenda a Instrução Normativa ME/SGD Nº 1/2019". Um terceiro participante indica que "*a gestão de riscos em aquisições de TIC deve ser planejada, estruturada, documentada e transparente para todos os envolvidos*".

A maioria dos participantes do questionário 2 afirmam que sua instituição não realiza a gestão de riscos em todas as fases da contratação. Verifica-se através dos relatos dos participantes o desconhecimento sobre como deve ser feita a gestão de riscos em aquisições de TIC. A figura 22 mostra a compilação das respostas obtidas na questão (6).

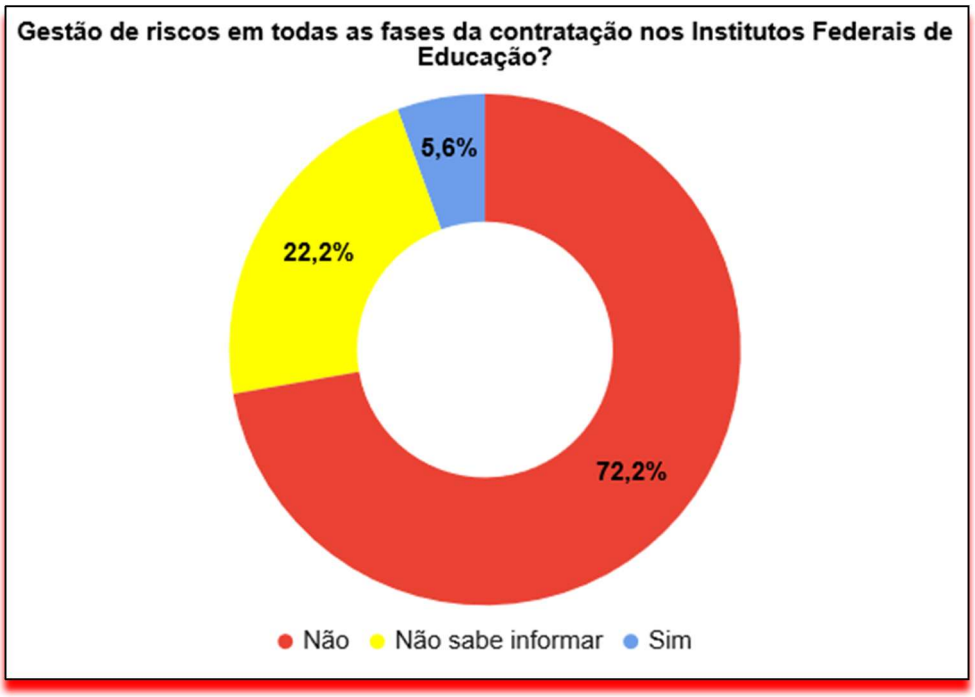


Figura 22 - Gestão de Riscos em Aquisições de TIC

Conforme apresenta a figura 22, 72,2% dos participantes deste estudo afirmam que sua instituição não adota procedimentos para realizar a gestão de riscos em todas as fases do processo de aquisições de TIC. Apenas 5,6 % dizem que adotam e 22,2% não souberam informar.

De forma a validar os resultados obtidos a partir do questionário 2, foram realizadas entrevistas em um Instituto Federal de Educação de forma a identificar quais são as barreiras e facilitadores para uso de uma solução para a gestão de riscos em aquisições de TIC. A próxima seção apresenta as informações compiladas.

4.2.3 Entrevistas: Barreiras e Facilitadores para uma Solução

A entrevista tem objetivo de obter informações a respeito de determinado assunto, utilizando uma conversação de natureza profissional (MARCONI, 2017). Yin (2015) afirma que a entrevista pode ser utilizada como uma fonte de informações para um estudo de caso.

As entrevistas foram realizadas no mês de agosto de 2019 com servidores do Instituto Federal de Educação, escolhido para o estudo de caso. As entrevistas foram previamente agendadas. A seleção de entrevistados foi feita com base na experiência em processos de aquisição de TIC. A finalidade das entrevistas realizadas nesta pesquisa foi validar as informações obtidas através dos questionários 1 e 2 de maneira a propor uma solução eficiente para gerir riscos em aquisições de TIC e que seja coerente com o contexto interno e externo das instituições públicas brasileiras.

Para isso, o público-alvo escolhido são os servidores que fazem parte da equipe de planejamento da contratação de TIC do Instituto Federal de Educação que será utilizado no estudo de caso. Oito servidores públicos participaram das entrevistas. Para manter suas identidades em sigilo foi definido um código aleatório para cada entrevistado. O perfil dos entrevistados encontra-se disponível no apêndice F.

A pesquisa adotou a técnica de entrevista estruturada em razão de possuir um roteiro estabelecido com perguntas a indivíduo previamente determinado (MARCONI, 2017; PROVDANOV; FREITAS, 2013). O roteiro da entrevista encontra-se disponível no apêndice E.

Após a comparação da solução indicada pelos participantes do questionário 2 (questão 18) e as sugestões feitas nas entrevistas (questão 6) é possível observar que a solução recomendada é a mesma, ou seja o uso de uma metodologia. No questionário 2, dos 18 participantes, 12 recomendaram a metodologia e nas entrevistas de 8 participantes, 5 indicam o uso da metodologia como solução para o problema da ineficiência em gerir riscos em aquisições de TIC.

Para que a gestão de riscos no processo de aquisição de TIC seja eficiente, segundo os participantes das entrevistas existem barreiras e facilitadores. De

acordo com os entrevistados, as barreiras que influenciam a eficiência da gestão de riscos em aquisições de TIC são apresentadas na figura 23.

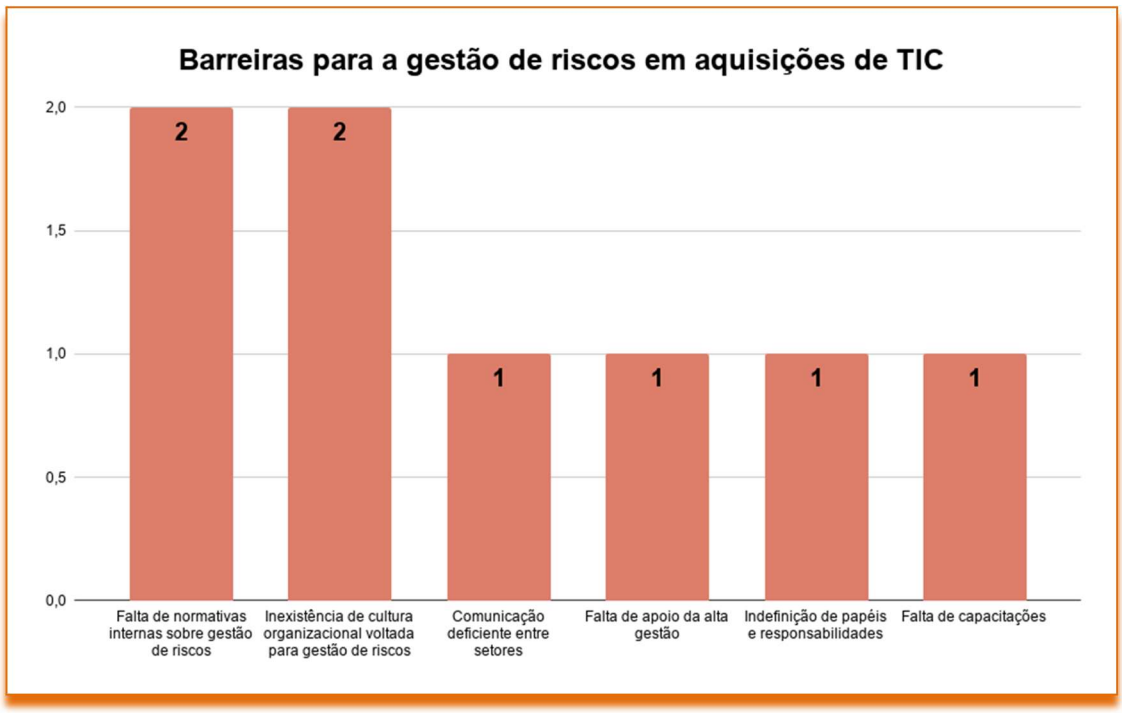


Figura 23 - Barreiras para a Gestão de Riscos em Aquisições de TIC

Conforme mostra a figura 23, para 2 dos participantes da entrevista que responderam a questão (7), a falta de normativas internas sobre gestão de riscos dificulta sua utilização no processo de aquisição de TIC. Outros 2 entrevistados afirmaram que quando a cultura organizacional não é voltada à gestão de riscos compromete o sucesso da iniciativa. Além disso, quando a comunicação entre os setores é deficiente dificulta o monitoramento e controle de riscos. A falta de apoio da alta gestão, a indefinição de papéis e responsabilidades e a falta de capacitações específicas em gestão de riscos torna o processo frágil.

Assim, como existem as barreiras que dificultam a realização de gestão de riscos eficiente no processo de aquisições de TIC, os entrevistados afirmam que existem varáveis que contribuem para o sucesso da iniciativa. A figura 24 apresentam as respostas obtidas na questão (8).

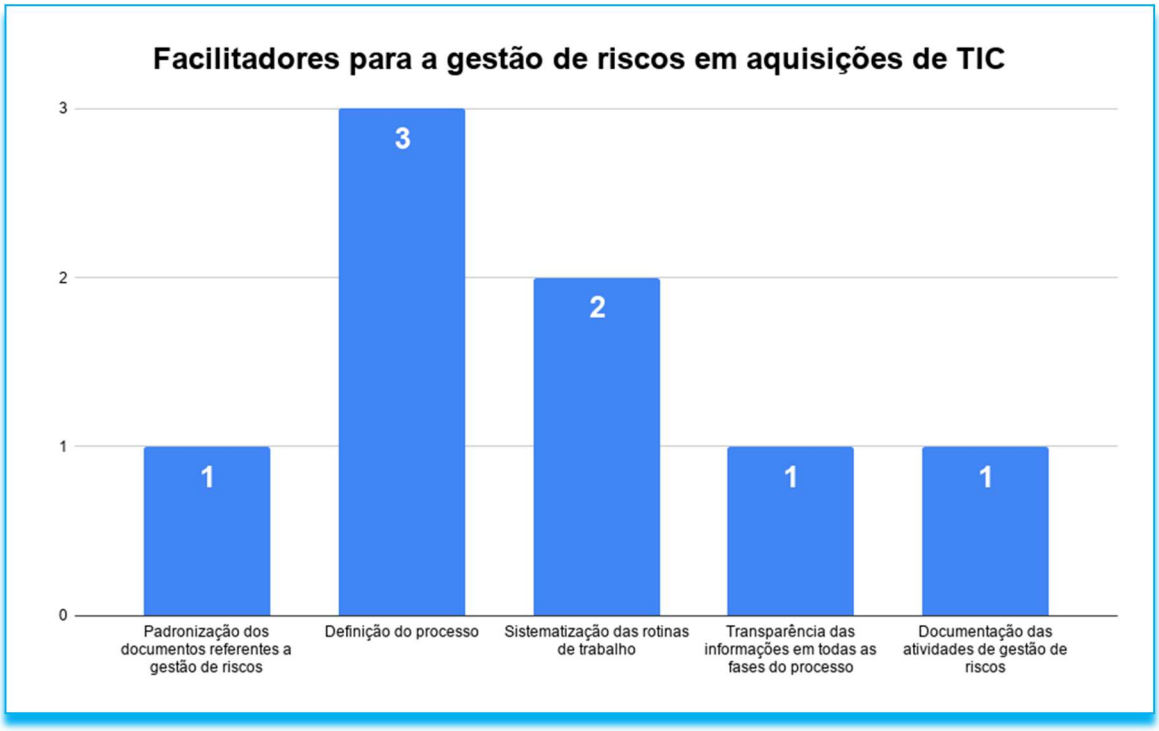


Figura 24 - Facilitadores para a Gestão de Riscos em Aquisições de TIC

Os entrevistados consideram como facilitadores para a eficiência da gestão de riscos em aquisições de TIC: a definição do processo de gestão de riscos, a sistematização das rotinas de trabalho, a transparência das informações em todas as fases do processo, a padronização dos documentos referentes a gestão de riscos e a documentação das atividades de gestão de riscos, conforme demonstra a figura 24. Como facilitador de maior influência, 3 entrevistados consideram a definição do processo de gestão de riscos.

4.3 CAUSAS PARA A DIFICULDADE EM GERIR RISCOS

Para definir as causas para a dificuldade em gerir riscos em aquisições de TIC de forma a compreender a deficiência apresentada pelas instituições públicas brasileiras, foram utilizados inicialmente os relatórios de governança pública do TCU (2017; 2018g). Além disso, foram realizados diversos procedimentos de coleta de dados (pesquisa bibliográfica, questionários, entrevistas e grupo focal). A compilação dos resultados obtidos está apresentada na figura 25.

Para a construção desta figura foram usadas informações coletadas através do questionário 1 (questão 16) correlacionadas com o questionário 2 (questão 23).

Em seguida, foi realizada a comparação com os resultados obtidos nos levantamentos de governança pública feitos pelo TCU nos últimos anos (TCU, 2017; 2018d). Também foram realizadas leituras de artigos científicos e dissertações sobre a temática aquisição de TIC, juntamente com pesquisa documental em relatórios de gestão, PDTI e planos de contratação.

A figura 25 mostra um diagrama de espinha de peixe apresentando algumas causas para a dificuldade em gerir riscos em aquisições de TIC. Para facilitar a compreensão, as causas foram categorizadas nas seguintes perspectivas: organização, processos, pessoas, comunicação, legislação e tecnologia.

Figura 25 – Causas-Raiz para Dificuldade em Gerir Riscos em Aquisições

A figura 25 apresenta causas-raiz para a dificuldade em gerir riscos em aquisições de TIC no setor público. Segundo os especialistas na área de TIC que preencheram o questionário 1 (questão 16) e questionário 2 (questão 23), as causas para o problema apresentado na figura 25, podem ser ocasionadas por diversos fatores. Na maioria das vezes estão relacionadas à falta de procedimentos operacionais padronizados que envolvem desde a organização, processos, pessoas, legislação, comunicação até tecnologia da informação.

Na perspectiva *organização* destacam-se as causas: inexistência de cultura organizacional voltada à gestão de riscos e a falta de padronização de

procedimentos para realização da gestão de riscos. Segundo um dos participantes do questionário 2, grande parte das instituições "*apenas identificam os riscos e não realizam o monitoramento e controle de seus riscos"*. Através de pesquisa documental nos sites institucionais dos Institutos Federais de Educação, apresentados no apêndice A, é possível verificar que alguns adotam um documento eletrônico contendo os riscos e as ações para tratamento. Outras instituições utilizam *checklists* para acompanhar apenas as atividades da etapa de planejamento da contratação.

Na perspectiva *processo,* a indefinição de como devem ser realizadas as atividades de gestão de riscos, acarreta na maioria das vezes atrasos na entrega dos bens, serviços ou produtos que comprometem o cumprimento dos objetivos organizacionais. Embora tenha a Instrução Normativa SGD/ME Nº 1/2019 que detalha a gestão de riscos em contratação de soluções de TIC, a Instrução Normativa Conjunta MP/CGU Nº 1/2016 e Instrução Normativa MPOG Nº 5/2017 que apresentam o processo a ser seguido para realizar a gestão de riscos, muitas das organizações públicas ainda não adotam as recomendações dos órgãos de controle (TCU, 2018e).

Em relação a *pessoas,* as causas prováveis para o problema relatado estão relacionadas à: indefinição de papéis, responsabilidades e rotinas de trabalho da equipe de planejamento da contratação, o que tem ocasionado a sobrecarga de atividades para alguns membros da equipe de planejamento da contratação. Segundo os participantes do questionário 1, muitas das vezes as causas estão relacionadas à falta de capacitação técnica da equipe.

Segundo os especialistas em TIC dos Institutos Federais de Educação que participaram do questionário 1, a *comunicação* entre os setores pode ser considerada uma das causas mais graves para a dificuldade em gerir riscos. A má comunicação envolvendo os atores do processo de aquisição de TIC pode dificultar ou comprometer a execução de atos administrativos relacionados a aquisições de TIC.

A falta de documentação referente ao processo compromete a transparência dos atos administrativos, o que dificulta a execução deste processo de negócio podendo acarretar na maioria das vezes atrasos no desenvolvimento de projetos de

ensino, pesquisa e extensão. Segundo 46,7% dos especialistas na área de TIC, participantes do questionário 1, suas instituições não divulgam todos artefatos que compõe o processo de aquisição e 33,3% publicam alguns. Apenas 3,3% apresentam todos os artefatos gerados durante o processo de aquisição de TIC.

Na perspectiva *tecnologia* uma causa que deve ser considerada, segundo os especialistas na área de TIC, participantes do questionário 1, está relacionada à inexistência de sistematização das atividades de monitoramento e controle que compõem a gestão de riscos. Alguns Institutos Federais de Educação possuem softwares excelentes para realizar a gestão de riscos, entretanto, somente utilizam para identificar riscos, não realizam o monitoramento e controle de riscos durante o processo de aquisição de TIC. Para alguns participantes do questionário 1 (questão 12), as atividades de gestão de riscos em aquisições de TIC não são acompanhadas de forma adequada.

Em relação à legislação observa-se que a equipe de planejamento de contratação embora realize diversos cursos de capacitação tem muitas dificuldades em especificar o termo de referência e o edital de forma que evite excessos de questionamentos e impugnações. Na maioria das vezes, segundo os especialistas na área de TIC, participantes do questionário 1, isto ocorre em razão do desconhecimento do que pode ser considerado como restrição à ampla concorrência ou direcionamento de fabricante.

4.4 REQUISITOS PARA A SOLUÇÃO A SER PROPOSTA

Os relatos apresentados nos questionários 1 e 2 juntamente com as entrevistas indicam que cada instituto federal de educação realiza a gestão de riscos do processo de aquisição de TIC de forma diferente, ou seja, cada um segue um padrão com procedimentos que na maioria das vezes não são transparentes para todos. Neste sentido, uma metodologia de gestão de riscos em aquisições de TIC que apresente procedimentos práticos, sistematizados e documentados de forma transparente em todas as fases da contratação pode ser uma solução para a ineficiência em gerir riscos em aquisições de TIC, podendo contribuir para agilizar a execução do processo.

Embora tenha a Instrução Normativa SGD/ME Nº 1/2019 que define que a gestão de riscos deve ser realizada em harmonia com a Política de Gestão de Riscos do órgão prevista na Instrução Normativa Conjunta MP/CGU Nº 1, de 10 de maio de 2016, a legislação vigente não apresenta de forma clara e objetiva como as atividades referentes à gestão de riscos devem ser conduzidas dentro do contexto das instituições públicas brasileiras. A figura 26 apresenta a sugestão de solução para o problema relatado neste estudo, feita pelos participantes do questionário 2, questão (18).

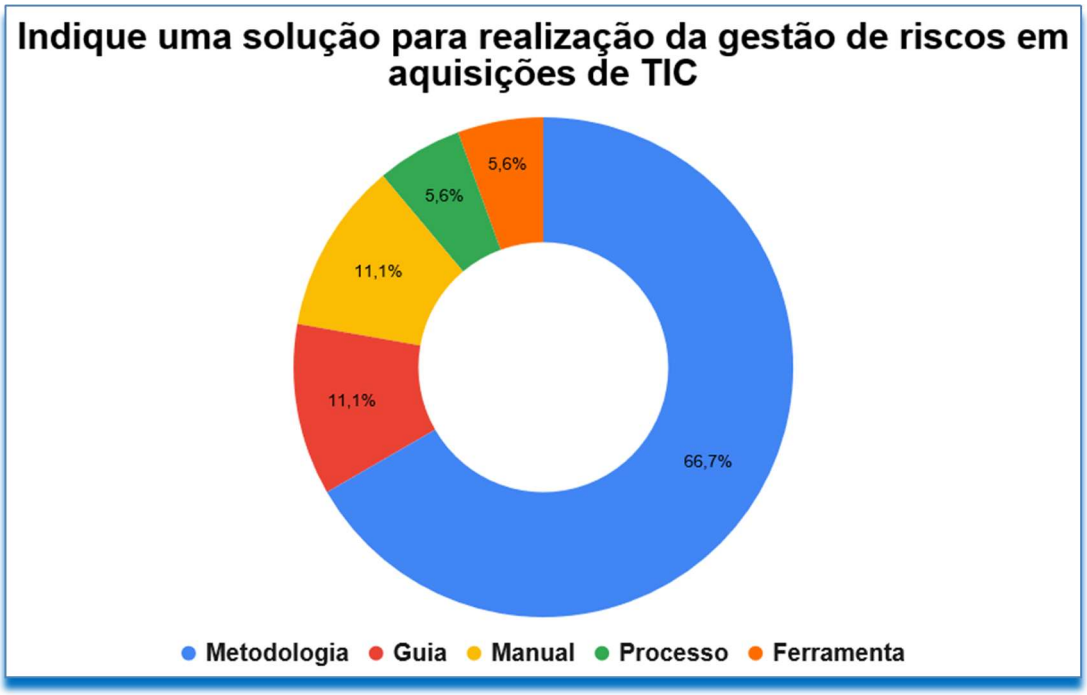


Figura 26 - Solução para Gestão de Riscos em Aquisições de TIC

Segundo a maioria dos participantes do questionário 2 (questão 18), conforme apresenta a figura 26, cerca de 66,7%, indicam que a solução mais indicada para realizar a gestão de riscos no processo de aquisição de TIC é uma metodologia. Em seguida, 11,1% sugerem um manual 11,1% indicam um guia, 5,6% uma ferramenta tecnológica e 5,6% afirmam que a definição do processo seria a sugestão mais indicada.

Um dos participantes do questionário 2 sugere que, a organização deve "*estabelecer uma metodologia para gestão de riscos relacionados a aquisições de TIC de forma que os riscos sejam identificados, avaliados, monitorados, relatados (documentados) e gerenciados de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus*

objetivos. Basicamente, seguir o COBIT 5, processo APO12 Manage Risk que define as principais práticas para a gestão de riscos". Outro complementa a "*necessidade de realizar monitoramento e controle contínuo de riscos em todas as fases do processo de contratação*". Vale ressaltar que a abordagem do COBIT não apresenta um detalhamento de como realizar a gestão de riscos no decorrer do processo de aquisição de TIC.

Já outro participante do questionário 2 afirma que "*como o aperfeiçoamento de todo processo de gestão de riscos é bem dinâmico e contínuo, sugere-se a padronização das fases de identificação, avaliação, tratamento, documentação e comunicação de riscos como alternativa para monitoramento e controle de riscos*". Para que isso seja possível, um participante considera que seja importante "*ter uma equipe ou setor que faça efetivamente o controle da gestão de riscos dentro da organização".*

Como forma para registro e relato das atividades a serem desenvolvidas em cada fase da gestão de riscos em aquisições de TIC, os participantes sugerem o uso de uma planilha eletrônica. A figura 27 apresenta as opções para registro de atividades citadas pelos participantes na questão (19), juntamente com o percentual de cada resposta.

Figura 27 – Ferramenta para Gestão de Riscos em Aquisições de TIC

A figura 27 apresenta a opinião dos participantes do questionário 2 em relação ao uso de uma ferramenta para registro de atividades sobre gestão de riscos em aquisições de TIC. Conforme pode ser verificado a maioria os participantes deste estudo, cerca de 50% sugerem o uso da planilha eletrônica como ferramenta para registro e relato das fases de identificação, avaliação, tratamento, monitoramento, controle e comunicação sobre riscos no processo de aquisição de TIC.

Diante destas constatações o próximo capítulo aborda o desenvolvimento da solução definida para estruturar, sistematizar e documentar de forma transparente a gestão de riscos no processo de aquisição de TIC. A solução apresentada no próximo capítulo foi construída a partir das sugestões feitas por especialistas na área que participaram dos questionários 1, 2 e entrevistas.

5 DESIGN DA SOLUÇÃO

O capítulo apresenta a proposição e especificação da solução para a ineficiência em gerir riscos no processo de aquisição de TIC no âmbito das instituições públicas brasileiras. Apresenta a metodologia de gestão de riscos GRATIC contendo o processo de gestão de riscos, técnicas, ferramentas, artefatos e procedimentos sistematizados.

5.1 DESENVOLVIMENTO DA SOLUÇÃO

A metodologia de Gestão de Riscos em Aquisições de TIC (GRATIC) é desenvolvida com base nas perspectivas: processo, pessoas, tecnologia, organização e legislação. A figura 28 sintetiza o que foi levado em consideração para o desenvolvimento da solução proposta neste estudo.

Figura 28 - Perspectivas para Desenvolvimento da Solução

A partir da figura 28 compreende-se que a perspectiva processo aborda como a gestão de riscos é realizada em aquisições de TIC, segundo a legislação vigente. Pessoas abrange os procedimentos adotados para realização das

atividades de gestão de riscos na prática em aquisições de TIC. A legislação aborda quais leis, decretos e instruções normativas são utilizados pelo governo federal para realizar a gestão de riscos nas aquisições de TIC. A organização detalha o que a organização já tem para realizar a gestão de riscos em aquisições de TIC. A tecnologia considera os recursos tecnológicos já utilizados no setor público para gerir riscos em aquisições de TIC.

5.2 METODOLOGIA GRATIC

A metodologia de gestão de riscos em aquisições de TIC (MGR-GRATIC) é estruturada em um ciclo iterativo e incremental dividido em quatro fases sequenciais inspiradas no ciclo de melhoria contínua PDCA (planejar, desenvolver, checar e agir). A MGR-GRATIC utiliza padrões consagrados sobre gestão de riscos tendo como objetivo, estabelecer e estruturar quatro fases para gerenciamento de riscos envolvendo aquisições de TIC.

A elaboração desta metodologia considera o contexto interno e externo das instituições públicas brasileiras, bem como a opinião de especialistas na área, participantes deste estudo. A proposta para gestão dos riscos no processo de aquisição de TIC da MGR-GRATIC é baseada nas recomendações publicadas na Instrução Normativa SGD/ME Nº 1 de 4 de abril de 2019, na Instrução Normativa MPOG Nº 5/2017 de 26 de maio de 2017 e na Instrução Normativa Conjunta MP/CGU Nº 1/2016 de 10 de maio de 2016.

A MGR-GRATIC utiliza técnicas, ferramentas, artefatos e procedimentos para a identificar, avaliar e a adotar respostas aos eventos de riscos, como também instrui sobre o monitoramento e controle, registro e reporte de riscos em aquisições de TIC. Para cada fase do processo de aquisição de TIC são executadas as quatro fases do processo de gestão de riscos de forma iterativa e incremental, uma vez que novos riscos podem aparecer durante a evolução do processo de aquisição de TIC.

Esta metodologia utiliza um inventário de riscos e controles, que já foram identificados por especialistas na área de aquisições de TIC para executar a fase 1 e 2, em seguida sequencialmente executa as fases 3 e 4, registrando as

informações na planilha documentadora (Mapa de Gerenciamento de Riscos) disponível no repositório digital de informações. A figura 29 apresenta a MGR-GRATIC.

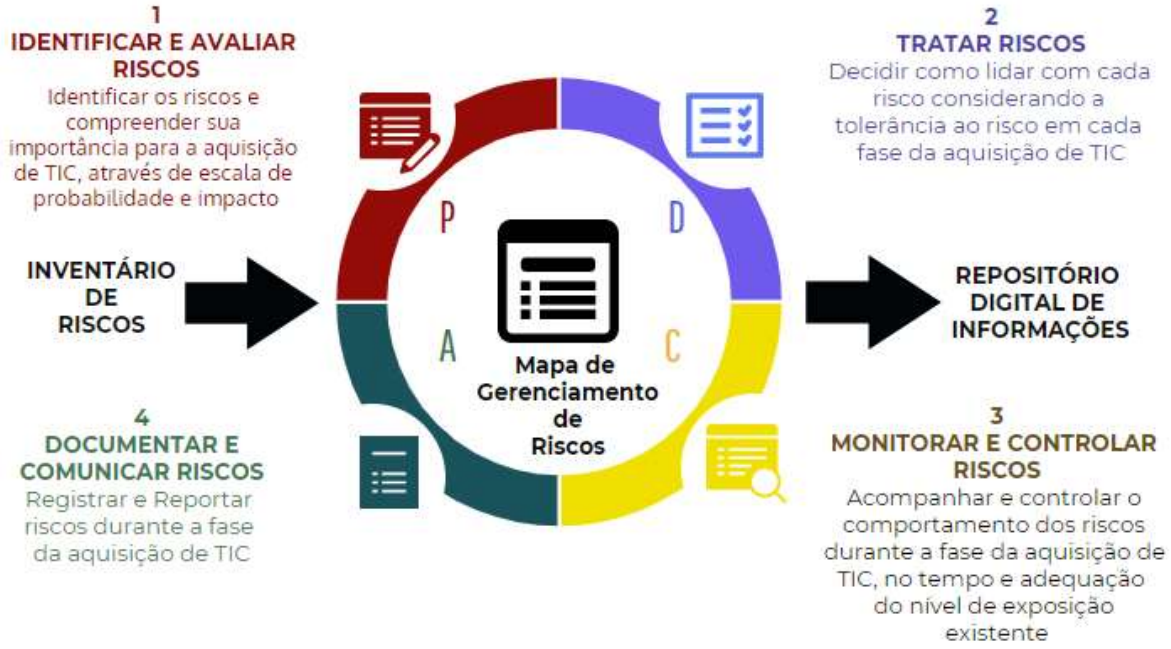


Figura 29 - MGR-GRATIC

A figura 29 apresenta a MGR-GRATIC composta por 4 fases baseadas no PDCA cujo objetivo é tornar os processos da gestão de uma empresa mais ágeis, claros e objetivos permitindo assim, o controle e melhoria contínua. Esta ferramenta de gestão é utilizada como referência em razão de ser um meio sistemático para análise e resolução de problemas, melhoria de resultados, como também alcance de metas e obtenção do comprometimento das pessoas.

A MGR-GRATIC adota boas práticas reconhecidas no mercado, apresentando características da estrutura dos componentes do *The Orange Book*, COSO ERM e ISO 31000. Na MGR-GRATIC os riscos são monitorados e controlados pela equipe de planejamento da aquisição.

A MGR-GRATIC se distingue das demais abordagens existentes no mercado, por disponibilizar um inventário contendo riscos e controles já identificados por especialistas na área, o que torna a identificação, análise,

avaliação e tratamento de riscos mais eficiente. A solução apresentada neste estudo utiliza práticas para monitoramento e controle de riscos de forma transparente aos envolvidos no processo de aquisições de TIC por meio de uma planilha documentadora disponibilizada em seu repositório digital de informações.

O diferencial da MGR-GRATIC em relação às outras existentes no setor público refere-se aos procedimentos práticos utilizados para identificação, análise, avaliação, tratamento, monitoramento, controle, comunicação e aprendizado sobre riscos em aquisições de TIC. Os artefatos disponibilizados além de tornar o processo mais ágil, possibilita o aprendizado contínuo e a transparência das atividades que envolvem a gestão de riscos.

Para ter o controle das fases da gestão de riscos em aquisições de TIC a MGR-GRATIC define papéis e responsabilidades para cada membro da equipe. Com isso, a gestão de riscos em aquisições de TIC torna-se planejada, averiguada e aperfeiçoada. A tabela 7 apresenta os papéis e responsabilidades de cada ator envolvido no processo.

Tabela 7 - Papéis e Responsabilidades

Fase	Ator	Responsabilidade
Planejamento da Aquisição	Equipe de planejamento do Aquisição	-Identificação e análise dos principais riscos que possam comprometer o sucesso da aquisição. -Mensuração das probabilidades de ocorrência e os danos potenciais relacionados a cada risco identificado. -Definição das ações a serem realizadas para eliminar ou minimizar as chances de ocorrência dos eventos relacionados a cada risco. -Definição das ações de contingência a serem tomadas caso os eventos correspondentes aos riscos se concretizem. - Definição dos responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência. -Registro e acompanhamento das ações de tratamento dos riscos. -Criação e atualização do mapa de gerenciamento de riscos.

Seleção do Fornecedor	Integrante Administrativo com apoio dos Integrantes Técnico e Requisitante	-Identificação e análise dos principais riscos que possam comprometer a seleção do fornecedor. -Avaliação e seleção da resposta aos riscos. -Registro e acompanhamento das ações de tratamento dos riscos. - Atualização contínua do Mapa de Gerenciamento de Riscos.
Gestão do Contrato	Gestor do Contrato	-Reavaliação dos riscos identificados nas fases anteriores e atualização de suas respectivas ações de tratamento. -Identificação, análise, avaliação e tratamento de novos riscos. -Atualização contínua do Mapa de Gerenciamento de Riscos.

A tabela 7 apresenta de forma detalhada os papéis e responsabilidades de cada ator envolvido e a fase do processo de aquisição de TIC. De acordo com a fase do processo existem atividades que devem ser realizadas para o controle de riscos.

5.2.1 Processo de Gestão de Riscos

O processo de gestão de riscos da MGR-GRATIC é baseado na norma ISO 31000, COSO, *The Orange Book* e está em conformidade com a Instrução Normativa complementar MP/CGU Nº 1/2016, Instrução Normativa MPOG Nº 5/2017 e Instrução Normativa ME/SGD Nº 1/2019. Ele é composto pelas fases: identificar e avaliar riscos, tratar riscos, monitorar e controlar riscos e documentar e comunicar riscos. A figura 30 apresenta o processo de gestão de riscos proposto pela MGR-GRATIC contendo suas fases e artefatos.

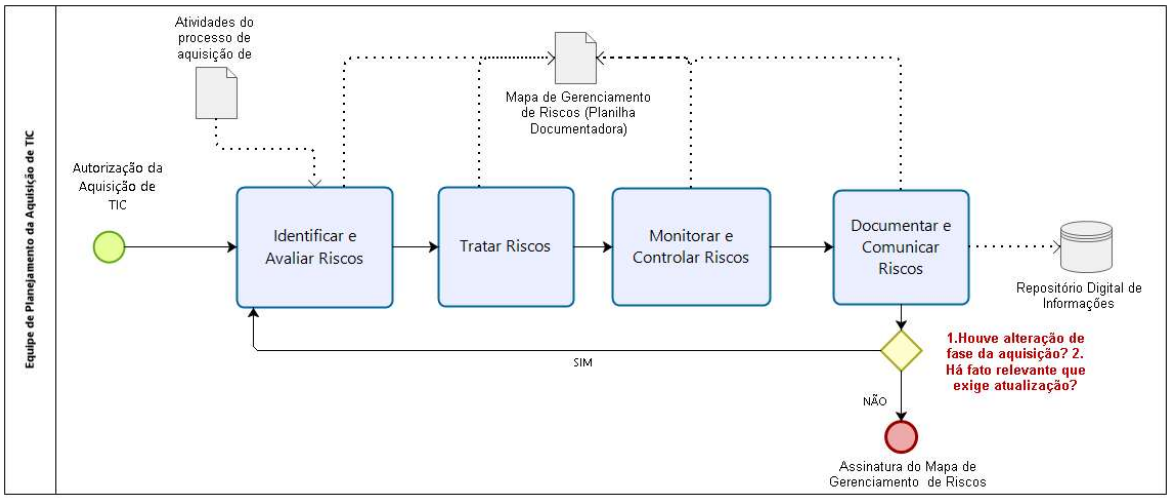


Figura 30 – Processo de Gestão de Riscos Proposto pela MGR-GRATIC

A figura 30 apresenta de forma sintetizada as fases que compõem o processo de gestão de riscos em aquisições de TIC proposto pela MGR-GRATIC bem como os artefatos utilizados para registro, comunicação, aprendizado e transparência sobre a gestão de riscos no processo de aquisição de TIC. Ressalta que para cada fase do processo de aquisição de TIC (planejamento da contração, seleção do fornecedor e gestão do contrato) deve ser realizado o ciclo completo de gestão de riscos proposto pela MGR-GRATIC.

As fases da MGR-GRATIC foram definidas a partir da revisão bibliográfica apresentada no capítulo 2 juntamente com sugestões feitas pelos participantes do questionário 2 e entrevistas realizadas com os especialistas na área de aquisições de TIC do Instituto Federal de Educação, utilizado como estudo de caso. As fases estão em conformidade com as abordagens existentes nos modelos de referência apresentados no capítulo 2. As quatro fases da MGR-GRATIC são:

Fase 1. Identificar e avaliar riscos: consiste em identificar e avaliar riscos e ameaças que possam vir a comprometer o sucesso da aquisição de TIC. Esta fase é responsável por compreender e analisar os riscos identificados para determinada aquisição de TIC, classificando-os em níveis de criticidade de acordo com a probabilidade e impacto de ocorrência dos mesmos. A figura 31 apresenta o detalhamento da fase 1.

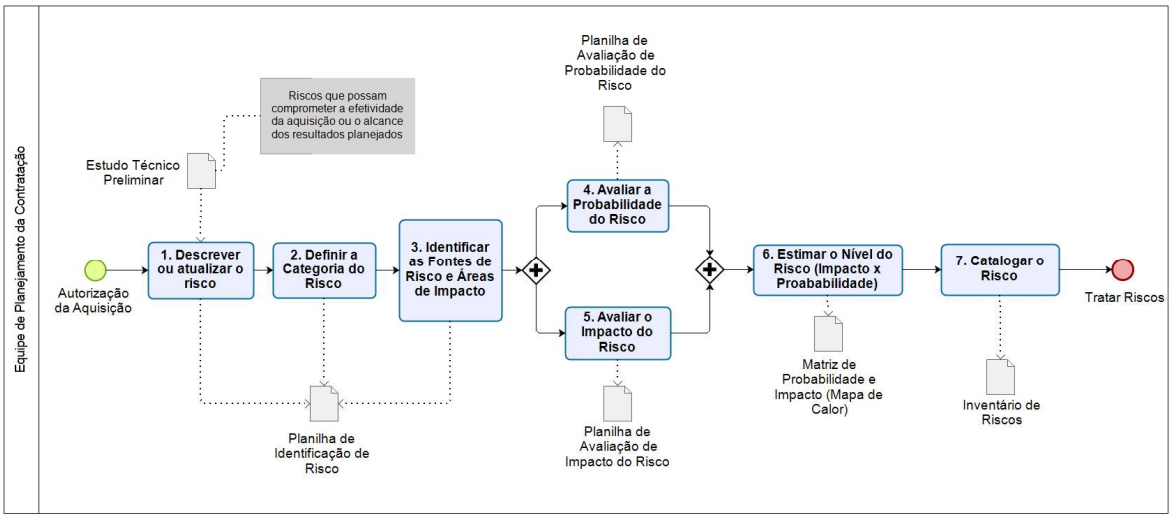


Figura 31 – Fase 1: Identificar e Avaliar Riscos

A fase 1 conforme mostra a figura 31 é composta por 7 atividades: descrever ou atualizar o risco, definir a categoria do risco, identificar as fontes de risco e áreas de impacto, avaliar a probabilidade do risco, avaliar o impacto do risco, estimar o nível do risco e catalogar o risco. A fase “Identificar e Avaliar Riscos” inicia com a autorização do processo de aquisição por parte da alta gestão da instituição e encerra com o início da fase 2 “Tratar Riscos”. A saída desta fase gera uma lista abrangente de riscos catalogada no inventário de riscos, baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da aquisição de TIC. A tabela 8 apresenta o detalhamento da fase 1.

Tabela 8 – Fase 1: Identificar e Avaliar Riscos

Objetivo	Identificar e avaliar riscos que possam comprometer a realização da aquisição de TIC.
Entradas	- Estudo técnico preliminar.
Técnicas	- Brainstorming - Entrevistas estruturadas e semiestruturadas - Questionários - Listas de verificação (*checklists*) - Matriz de probabilidade e impacto - Opinião especializada (PMI, 2013 e 2017)
Detalhamento da fase	1. Descrever ou atualizar os principais riscos/eventos que possam comprometer o sucesso da aquisição de TIC e de gestão contratual (descrição, proprietário do risco, causa do risco, efeito/dano/consequência e qual fase da aquisição ocorre). O apêndice J apresenta o inventário de riscos da aquisição de TIC proposto pela MGR-GRATIC (Brasil, 2019c). 2. Definir a categoria a qual o risco pertence: conformidade, estratégico, operacional, orçamentário, reputação e integridade. 3. Identificar as áreas de impacto: TI, RH, processo, organização, legislação e comunicação.

	4. Avaliar a probabilidade de ocorrência do risco a partir da descrição do risco, a medida de controle, tipo de controle existente, maturidade do controle e área afetada. A matriz utilizada para avaliar a probabilidade proposta pela MGR-GRATIC está disponível no apêndice K (Brasil, 2019c). 5. Avaliar o impacto do risco para a aquisição de TI com base no cálculo do nível de impacto. O apêndice L apresenta a planilha utilizada para realizar o cálculo de nível de impacto (IRM, 2002). 6. Estimar o Nível do Risco: construir a matriz de probabilidade x impacto (mapa de calor) com delimitações dos riscos aceitáveis para o processo de aquisição de TIC. O apêndice M apresenta a matriz de probabilidade e impacto utilizada pela MGR-GRATIC. 7. Catalogar o Risco.
Responsável	Integrante Técnico (Área de Tecnologia da Informação) Integrante Administrativo (Área Administrativa)
Saídas	- Lista contendo inventário de riscos para a aquisição de TIC. O apêndice J apresenta a lista de riscos em aquisições de TIC, disponibilizada pela MGR-GRATIC. - Planilha de identificação de risco. - Planilha de avaliação de probabilidade de risco. - Planilha de avaliação de impacto de risco. - Matriz de probabilidade x impacto dos riscos da aquisição de TIC. O apêndice M apresenta o mapa de riscos utilizado pela MGR-GRATIC.

Práticas recomendadas:
1. Entender o contexto (CGU, 2018).
2. Utilizar a matriz de SWOT para analisar contexto (BERMEJO et al., 2019).
3. Adotar uma visão de portfólio de risco, ou seja classificar riscos em categorias previamente definidas. Os riscos devem ser agrupados de acordo com suas causas: estratégicos, operacionais, legais, financeiros, tecnológicos entre outros (COSO, 2017; IN 1/2016).
4. Construir e manter atualizado o inventário de riscos e controles aplicados (COSO, 2004).
5. Utilizar os riscos que estão presentes no inventário de riscos existentes na planilha documentadora proposta pela MGR-GRATIC.
6. Definir papéis e responsabilidades, taxonomia de eventos de riscos e lista de controles básicos (MGR-GIRC, 2017).
7. Utilizar técnicas de avaliação de riscos para identificar e avaliar os riscos da aquisição de TIC, são elas: *brainstorming*, entrevistas estruturadas e semiestruturadas, listas de verificação e questionários recomendados pela ISO 31010 (2019) e HMG (2019).
8. Construir o mapa de riscos (MPOG, 2016), (MPOG, 2017b).
9. Utilizar a matriz de risco (probabilidade x impacto) para avaliar o nível de criticidade do risco (HMT, 2004), (PMI, 2013 e 2017), (HMG, 2019) e (IBGC, 2017).
10. Utilizar a escala de probabilidade e impacto para avaliar riscos (CGU, 2018), (IRM, 2002). Utilizar as escalas definidas pela metodologia GRATIC.
11. Utilizar planilha documentadora para identificar riscos (MPOG, 2017b).
12. Identificar os riscos através de oficinas de trabalho, *workshops* e reuniões (PMI, 2013 e 2017), (TCU, 2018b). Recomenda-se que as reuniões sejam realizadas mensalmente e preferencialmente a cada término da fase do processo de contratação de TIC.
13. Utilizar opinião especializada (idealmente de especialistas com experiência relevante e recente) é necessária para identificar os impactos potenciais no custo e no cronograma, avaliar a probabilidade e para definir entradas, tais como distribuições de probabilidades (PMI, 2013 e 2017).

Recomenda-se fortemente que na fase 1, descrita na tabela 8 sejam realizadas reuniões entre os membros da equipe de planejamento da aquisição de TIC e equipe de apoio (área administrativa) de forma a construir o inventário de riscos e matriz de probabilidade x impacto com auxílio de *checklist*, apresentando

uma lista com fontes de riscos já conhecidas e atualizadas pelos órgãos de controle (TCU, 2013). O mapa de gerenciamento de riscos, disponibilizado no apêndice H apresenta uma lista com riscos e controles já identificados em outros projetos relativos a aquisições de TIC, o que contribui para tornar o processo de identificação de riscos mais produtivo.

Caso seja necessário, a equipe de planejamento da aquisição pode consultar outros setores para resolução de dúvidas e coleta de informações necessárias para “Identificar e Avaliar os Riscos”. A MGR-GRATIC descreve em seu manual, disponibilizado no apêndice H, como avaliar a gravidade de cada risco e a prioridade para tratamento.

Ela disponibiliza uma matriz de probabilidade e impacto, baseada no *The Orange Book* do governo britânico, a qual verifica o nível de priorização dos riscos para uma posterior análise das respostas (HMT, 2004). Na MGR-GRATIC o risco possui uma descrição, proprietário, causa, efeito/dano/consequência, categoria e fase da contratação.

A tipificação dos riscos visa assegurar a definição de uma linguagem comum para riscos, considerando a descrição ampla dos tipos de riscos. Neste sentido, os riscos referentes às fases do processo de aquisição de TIC são identificados e agrupados em categorias de acordo com o nível de impacto e nível de tolerância.

Na MGR-GRATIC os riscos são rotulados e analisados de acordo com os seus tipos, ou seja a natureza do fato que gera o risco. Há uma variedade de fatos que geram riscos no ambiente organizacional e quando se pesquisa o tipo de risco deve-se atentar para os efeitos gerados pela concretização do risco. Nesse sentido, as ações e seus riscos associados são classificados de acordo com suas características.

Os tipos de riscos estabelecidos na MGR-GRATIC foram definidos a partir da tipologia apresentada pela metodologia do Ministério de Planejamento, Orçamento e Gestão (MPOG, 2017), CGU (2018) e orientação da Instrução Normativa Conjunta MP/CGU Nº 1/2016. Estas definições permitem conhecimento e análise crítica dos riscos institucionais e contribui para maior

objetividade das análises quanto aos impactos. A tabela 9 apresenta a taxonomia adotada pela MGR-GRATIC.

Tabela 9 – Taxonomia de Riscos

Tipo/Categoria	Descrição
Imagem/Reputação	Eventos que podem comprometer a confiança da sociedade em relação à capacidade da instituição em cumprir sua missão institucional. Risco de perda resultante de danos à reputação da organização, em perda de receita, aumento de custos operacionais, de capital ou destruição do valor, causado por um evento adverso ou potencialmente criminoso, mesmo que a instituição não seja culpada.
Financeiro/Orçamento	Eventos que podem comprometer a capacidade da instituição de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações (CGU, 2018). Diz respeito à possibilidade das receitas e despesas previstas não se confirmarem, isto é, durante a execução orçamentária ocorram desvios entre receitas e despesas orçadas.
Legislação/Conformidade	Eventos provenientes de alterações legislativas ou normativas que podem vir a comprometer as atividades da instituição (CGU, 2018). Engloba possíveis perdas por documentação insuficiente, insolvência, ilegalidade, falta de representatividade e/ou autoridade. Estão relacionados ao cumprimento da legislação e/ou regulamentação aplicáveis ao negócio e às normas e procedimentos internos.
Operacional	Eventos, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, que podem comprometer as atividades da instituição, podendo afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público (CGU, 2018).
Estratégico	Afeta a estratégia de negócio ou os objetivos estratégicos de uma organização. Podem ser incertezas ou oportunidades e normalmente são os principais pontos de preocupação da alta gestão.
Integridade	Evento relacionado à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pela instituição e a realização de seus objetivos (CGU, 2018).

Com base na tipologia/categoria do risco conforme apresenta a tabela 9 é realizada a análise de riscos. Na análise dos riscos são definidos os tipos de controle para cada risco de acordo com o nível de maturidade da instituição em

relação ao controle a ser adotado. Os tipos de controle são: corretivo, detectivo e preventivo.

Controle preventivo diz respeito a levantar quais ações podem ser realizadas visando a prevenção de possíveis causas de riscos (intencionais ou não). Controle corretivo apresenta medidas que podem ser executadas quando um risco já foi causado. Controle detectivo visa a identificação de um erro ou irregularidade depois que este tenha ocorrido.

A qualidade e a credibilidade da análise dos riscos requerem a definição de diferentes níveis de probabilidade e impacto dos riscos que são específicos ao contexto do projeto (PMI, 2013). A tabela 10 apresenta a escala de níveis de controle com suas respectivas probabilidades.

Tabela 10 – Escala de Tipos de Controle de Risco

Tipo de Controle	Nível de Maturidade	Probabilidade de ocorrer o risco
Corretivo	Inexistente	Elevada
	Fraco	Muito Alta
Detectivo	Insatisfatório	Alta
Preventivo	Satisfatório	Média
	Forte	Baixa

A partir da definição do tipo de controle a ser aplicado a cada risco de acordo com a escala estabelecida na tabela 10, é feita a avaliação de forma a verificar o nível de controle a ser adotado. Para realizar esta atividade a MGR-GRATIC utiliza as recomendações contidas no manual de gestão de riscos divulgado pelo TCU em 2018 (TCU, 2018).

A MGR-GRATIC usa uma matriz de probabilidade e impacto, baseada no *The Orange Book* do governo britânico, que verifica o nível de priorização dos riscos para uma posterior análise das respostas (HMT, 2004). A matriz define o nível de riscos a partir da combinação das escalas de probabilidade e de impacto.

A probabilidade consiste no resultado da materialização de um dado risco em determinado horizonte de tempo. É a chance do evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado. Por exemplo, se o objeto da gestão de riscos é uma aquisição de computadores, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final.

As escalas podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade. Na MGR-GRATIC são utilizadas escalas qualitativas de probabilidade com amplitude de até cinco níveis: baixa, média, alta, muito alta e elevada.

O Cálculo da probabilidade é feito a partir da **média aritmética** entre os seis macro fatores de riscos (TI, RH, Processos, Organização, Legislação, Comunicação) acrescidos da exposição ao risco (elevada, muito alta, alta, média e baixa). Então, se obtém um número para a classificação da probabilidade do risco (baixa, média, alta, muito alta e elevada), para cada risco identificado, conforme demonstra a tabela 11.

Tabela 11 - Escala de Probabilidade de Ocorrência do Risco

Probabilidade	Descrição	Peso
Baixa	Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	<=20
Média	De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	<=40
Alta	De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	<=60
Muito Alta	De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	<=75
Elevada	Praticamente certa. De forma inequívoca, o evento ocorrerá as circunstâncias indicam claramente essa possibilidade.	>75

A tabela 11 apresenta a escala de probabilidade adotada pela MGR-GRATIC que define a probabilidade de forma quantitativa de acordo com o peso definido. Esta escala foi sugerida por especialistas na área de contratações de TIC do Instituto Federal de Educação, utilizado no estudo de caso.

O cálculo do impacto consiste no resultado da materialização de um dado risco, medido por critérios preferencialmente quantitativos. A avaliação do impacto é feita a partir da **média ponderada** entre as áreas afetadas imagem, financeiro, legislação e operacional.

De acordo com os valores informados nas categorias (imagem, financeiro, legislação e operacional) é realizada uma média que define o nível de impacto do

risco para a fase da aquisição de TIC. Com isso, obtém-se o número indicativo do nível de impacto (baixo, médio, alto, muito alto e elevado), para cada risco identificado.

A avaliação da relevância do impacto dos riscos em cada fase da aquisição é realizada através da relevância do impacto em cada área (imagem, financeiro, legislação e operacional) conferindo uma nota ao impacto. Essa nota poderá se abrandar ou agravar a nota de acordo com o nível de tolerância (tempo) à ação saneadora. A MGR-GRATIC é capaz de aferir o nível de impacto de cada processo crítico de trabalho (alto, médio, baixo, leve, muito leve) e conferir um status de criticidade (crítico, moderado, leve) a cada processo de trabalho vulnerável.

Na MGR-GRATIC optou-se por definir uma escala adaptada da metodologia de gestão de riscos SISP (MPOG, 2017) para realizar o cálculo do nível de impacto. O impacto varia de acordo com a área impactada. Quando um risco impactar mais de uma área, deverá ser usada a área mais impactada.

Este cálculo é realizado para definir o nível de tolerância a riscos. Para definir o impacto dos riscos a MGR-GRATIC define uma escala contendo pesos. De acordo com o valor atribuído ao peso é definido o impacto do risco. A tabela 12 apresenta a definição dos pesos adotados para cálculo de impacto de riscos. A escala de impacto é definida em muito baixo (1), baixo (2), médio (3), alto (4) e muito alto (5):

Tabela 12 - Escala de Impacto do Risco

Impacto	Descrição	Peso
Muito baixo (1)	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	<=1.5
Baixo (2)	Pequeno impacto nos objetivos	<= 2.5
Médio (3)	Moderado impacto nos objetivos, porém recuperável.	<= 3.5
Alto (4)	Significativo impacto nos objetivos, de difícil reversão	< = 4.5
Muito Alto (5)	Catastrófico impacto nos objetivos (idem), de forma irreversível.	> 4.5

A tabela 13 apresenta a pontuação de impacto utilizada pela MGR-GRATIC. A pontuação é definida de acordo com as áreas da organização. Os pesos foram

definidos de acordo com o nível de tolerância para o risco. A pontuação de impacto foi baseada em IRM (2002).

Tabela 13 - Pontuação para Escala de Impacto do Risco

Pontuação	Escala				
	Imagem	Financeiro	Legislação	Operacional	Nível de Tolerância
5	De caráter internacional	Massivo	Perturbações muito graves	Perturbações muito graves	Muito alto
4	De caráter nacional	Severo	Graves	Graves	Alto
3	Regional	Moderado	Limitadas	Limitadas	Médio
2	Local	Leve	Leves	Leves	Baixo
1	De caráter individual	Insignificante	Muito leves	Muito leves	Muito baixo

A pontuação apresentada na tabela 13 leva em consideração o nível de tolerância. O resultado da avaliação dos riscos entre probabilidade versus impacto de sua ocorrência é representado através da Matriz de Riscos. Os riscos possuem limites de exposição. Para apresentar os limites adota a convenção apresentada na tabela 14.

Tabela 14 – Faixas de Nível de Risco

Faixa	Nível
Vermelha	Muito alto (Transferir - Altíssima exposição)
Laranja	Alto (Evitar - Alta exposição)
Amarela	Médio (Mitigar - Média exposição)
Verde	Baixo e muito baixo (Aceitar - Baixa exposição)

Os níveis de riscos identificados na tabela 14 são posicionados na matriz de acordo com a avaliação realizada de probabilidade de ocorrência e impacto. Os riscos podem diferir também em nível de urgência. Irá variar com relação ao tempo de antecedência com que precisam ser tratados e também ao tempo necessário para resposta. Dois riscos de mesma probabilidade e impacto podem ter níveis de urgência de tratamento diferentes. Uma escala complementar para o nível de urgência deverá ser criada para auxiliar a análise levando este fato em consideração.

Após identificação e avaliação de riscos, sua priorização se dará pela maior relação entre impacto e probabilidade, estabelecendo assim o grau de exposição ao risco e que orientará a prioridade de acompanhamento periódico. A figura 32 apresenta a matriz de probabilidade e impacto utilizada pela MGR-GRATIC. A matriz de riscos é uma adaptação do *The Orange Book* (HMT*, 2004)*.

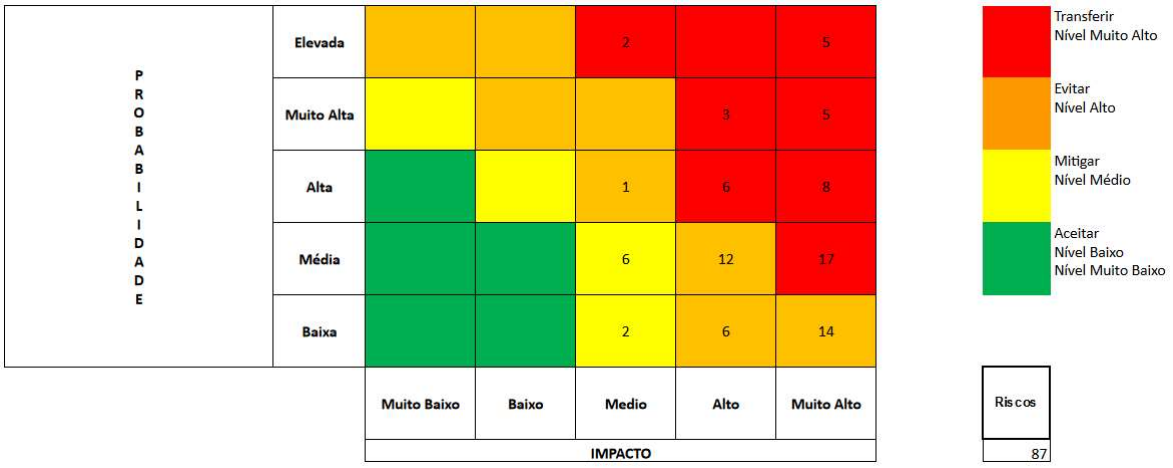


Figura 32 – Matriz de Probabilidade e Impacto do Risco

Uma vez que os riscos foram identificados e avaliados, a atividade subsequente é a priorização dos riscos para o tratamento. A priorização de riscos é feita a partir do cálculo de nível de impacto apresentado na matriz de probabilidade e impacto semelhante ao modelo apresentado na figura 32. Na fase 2 são definidas atitudes perante os riscos a serem tratados de acordo com o nível de impacto para o processo de aquisição de TIC.

Fase 2.Tratar Riscos: consiste em definir a resposta, comparando os resultados encontrados com os critérios para tratamento de riscos previamente definidos e determina se o risco identificado exige tratamento. Esta fase contempla a elaboração de respostas aos riscos, com o objetivo de reduzir as ameaças levantadas.

A norma ISO 31000 (2018) detalha que as opções de tratamento de riscos não são necessariamente adequadas em todas as circunstâncias, deve-se verificar risco a risco para aplicação necessária dos controles. A figura 33 apresenta o detalhamento da fase 2.

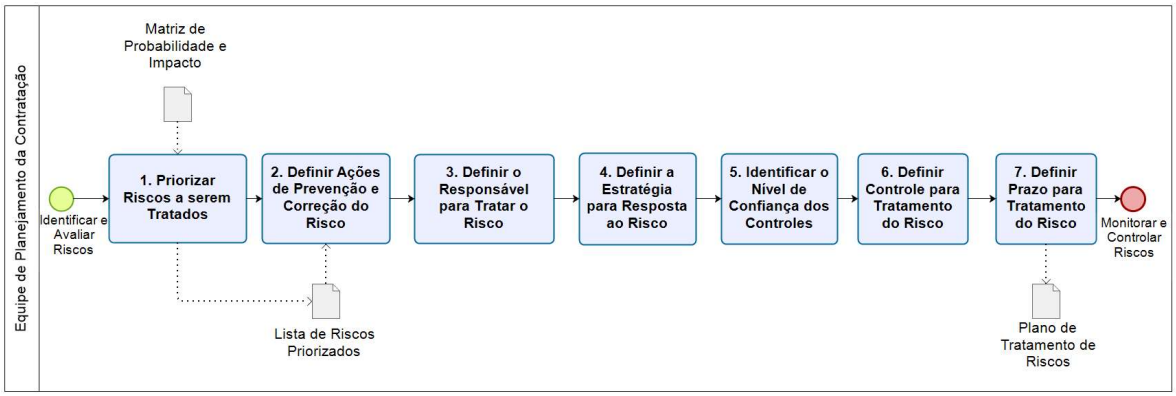


Figura 33 – Fase 2: Tratar Riscos

A fase 2 da MGR-GRATIC apresentada na figura 33 é composta por 7 atividades: priorizar riscos a serem tratados, definir ações de prevenção e correção do risco, definir o responsável por tratar o risco, definir a estratégia para resposta ao risco, identificar o nível de confiança dos controles, definir controle para tratamento do risco e definir prazo para tratamento do risco. A fase 2 inicia quando a identificação e avaliação de riscos com base na matriz de probabilidade e impacto de cada risco é encerra com o início da fase 3 “Monitorar e Controlar Riscos” a partir do plano de tratamento de risco. Dentro do contexto apresentado, a tabela 15 apresenta o detalhamento da fase 2.

Tabela 15 – Fase 2: Tratar Riscos

Objetivo	Criar e utilizar um plano de ação para tratamento de riscos da aquisição de TIC.
Entradas	- Matriz de probabilidade e impacto.
Técnicas	- Opinião especializada (PMI, 2013 e 2017).
Detalhamento da fase	1. Priorizar riscos a serem tratados (lista de riscos priorizados). 2. Definir as ações de prevenção e correção do risco. 3. Definir o responsável para tratar o risco da aquisição de TIC. 4. Definir a estratégia para resposta ao risco: mitigar, transferir, aceitar e evitar (HMT, 2004). 5. Identificar o nível de confiança dos controles. 6. Definir o controle para tratamento do risco da aquisição de TIC (MPOG, 2016): detectivo, corretivo ou preventivo. 7. Definir prazo para tratamento do risco.
Responsável	Integrante Técnico Integrante Administrativo
Saídas	- Lista de riscos priorizados. - Plano de tratamento de riscos (MPOG, 2016).

Práticas recomendadas:
1. Definir um plano de resposta ao risco (OGC, 2010), (MPOG, 2016), (ISACA, 2013), (PMI, 2013 e 2017) e (CGU, 2018).
2. Realizar abordagem estrutural para tratamento de riscos conforme a priorização de riscos de acordo com as camadas da pirâmide de riscos do framework 4A (Westerman e Hunter, 2008).
3. Priorizar riscos a serem tratados (CGU, 2018), (TRT, 2017) e (TRE-PA, 2018).
4. Definir formas para tratar riscos (CGU, 2018).
5. Definir controles para tratamento de riscos (MPOG, 2016).
6. Definir um relatório de progresso do tratamento do risco (OGC, 2010) e (CGU, 2018).

A tabela 15 apresenta as atividades desenvolvidas na fase 2 da MGR-GRATIC. Os riscos identificados e analisados na fase de identificar e avaliar riscos são insumos para a fase tratar riscos. Os registros dos riscos são desenvolvidos incrementalmente ao longo da execução do processo de aquisição de TIC.

Cada risco identificado terá seu devido planejamento de resposta, criando assim um inventário de risco também para os controles e tratamentos definidos. A norma ISO 31000 (2018) recomenda que se não houver opções de tratamento de riscos disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, convém que este seja registrado e mantido sob análise crítica.

O tratamento de riscos na MGR-GRATIC segue uma priorização, com base na avaliação do grau de exposição, e pode utilizar uma ou mais alternativas de tratamento. As opções de tratamento utilizadas são baseadas no *The Orange Book*: mitigar, transferir, eliminar e aceitar (HMT, 2004).

A equipe de planejamento da aquisição deve escolher as respostas aos riscos, ou seja deve desenvolver uma série de medidas para alinhar os riscos com tolerância e com o apetite a risco. A MGR-GRATIC utiliza as opções de resposta a riscos inspiradas no PMBOK (PMI, 2013) e CGU (2018), conforme mostra a tabela 16.

Tabela 16 – Tipo de Respostas para Riscos

Resposta	Descrição
Transferir	A organização transfere o risco para uma terceira parte. Ocorre quando o risco é classificado como muito alto.
Evitar	Utilizada para riscos classificados como alto, ou seja, que apresentem um controle com uma relação custo x benefício muito elevado. Reduz a zero a probabilidade de ocorrência do evento de risco.
Mitigar	São implementadas ações que visem reduzir as causas ou consequências do risco até um nível aceitável. Este tipo de resposta é utilizado para riscos classificados como médio.
Aceitar	O risco é aceito e nenhum novo controle precisa ser implementado para mitigar o risco. Esta resposta é utilizada para riscos na faixa aceita de apetite de riscos. Nenhuma ação é realizada pois o nível é baixo.

A tabela 16 apresenta as opções de tratamento propostas pela MGR-GRATIC: transferir, evitar, mitigar e aceitar. O tratamento de risco é realizado a partir da ferramenta 5W2H, também utilizada na construção de listas de verificação para monitoramento e controle de riscos.

O planejamento para resposta ao risco é feito através do *plano de tratamento de riscos.* O responsável por cada risco deve propor a respectiva resposta ao risco. Uma vez definida a resposta a ser dada ao risco, a mesma é incluída no plano de tratamento de riscos.

Para todos os riscos prioritários devem ser elaborados preventivamente respostas com as medidas a serem adotadas em caso de materialização do risco. O plano de tratamento de respostas a riscos utilizado pela MGR-GRATIC encontra-se disponível no apêndice N.

As atualizações ou registro dos controles devem ser validadas continuamente no plano de tratamento de riscos. Alguns indicadores de desempenho são indicados, como a verificação das ações corretivas e sua efetividade no objetivo de controles e andamento no cronograma da aquisição de TIC.

Identificados os riscos, tendo-os analisados, classificados por criticidade e definidas as ações com os controles e respostas a serem realizadas é preciso ter o controle sobre as ações planejadas, monitorar o comportamento dos riscos ao longo da execução do processo licitatório. A próxima fase ‘Monitorar e Controlar Riscos” trata especificamente da garantia da eficiência da gestão de riscos no processo de aquisição de TIC.

Fase 3. Monitorar e Controlar Riscos: consiste em monitorar o comportamento dos riscos ao longo do tempo de execução do processo de aquisição de TIC. Verifica se os riscos ainda existem e realiza o controle quanto à adequação do perfil de tolerância aos riscos definidos pela instituição.

O monitoramento dos riscos na MGR-GRATIC tem o objetivo de avaliar a efetividade do processo de gestão de riscos e dos controles internos, por meio de atividades gerenciais contínuas, buscando assegurar seu funcionamento como definido e identificar oportunidades de aprimoramento, em conformidade com as mudanças nas condições que alterem o nível de exposição aos riscos. Neste

sentido, inclui tomar as medidas de correção que se mostrarem necessárias na revisão do plano de tratamento de riscos.

A fase 3 é responsável por atualizar os registros e documentos gerados durante a aquisição de TIC. Isto garante que a gestão de riscos esteja sendo efetivamente realizada em todas as fases do processo de aquisição. O monitoramento e controle de riscos visa analisar informações coletadas (ações de controle) de forma a corrigir falhas durante a execução do processo de aquisição de TIC. Esta atividade é realizada em reuniões mensais através de *checklists*.

Na MGR-GRATIC há a definição clara e objetiva de listas de verificação e relatórios de revisão para que as ações de monitoramento e controle de riscos sejam efetivas. Para isso, utiliza planilhas de acompanhamento e controle que estão disponibilizadas nos apêndices I, O, P, Q e R.

Durante as reuniões de acompanhamento devem ser verificados elementos como: se novos riscos apareceram, se a probabilidade e/ou impacto dos riscos mudaram, reportar aos níveis adequados e mudanças significativas que alteram o nível de riscos. O registro de monitoramento e controle de riscos em aquisições de TIC devem ser realizados em todas as fases da contratação de TIC. A figura 34 apresenta a fase 3 “Monitorar e Controlar Riscos”.

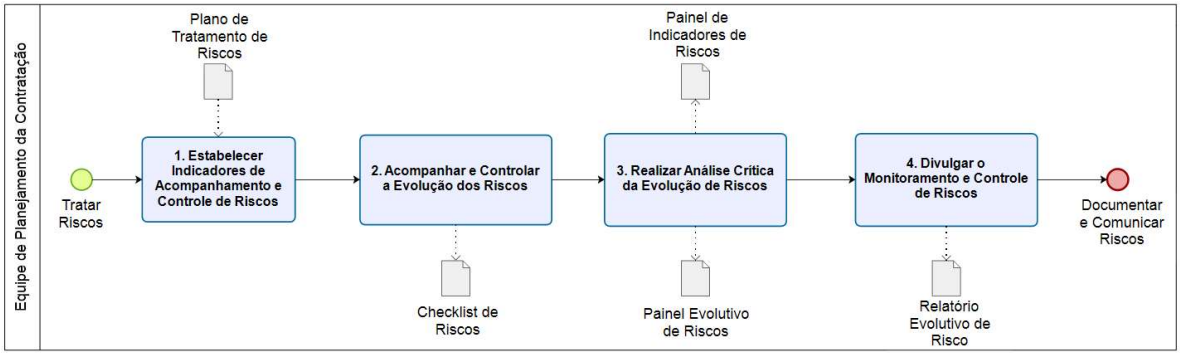


Figura 34 – Fase 3: Monitorar e Controlar Riscos

A figura 34 mostra como a fase 3 é executada. Ela é composta por 4 atividades: estabelecer indicadores de acompanhamento e controle de riscos, acompanhar e controlar a evolução dos riscos, realizar análise crítica da evolução de riscos e divulgar o monitoramento e controle de riscos. A fase 3 inicia com o término da fase “Tratar Riscos” com o uso do plano de tratamento de riscos e

encerra com a divulgação do relatório evolutivo de risco com o início da fase “Documentar e Comunicar Riscos”.

A fase 3 é considerada uma das fases mais importantes para a eficiência da gestão de riscos em aquisições de TIC na MGR-GRATIC, uma vez que monitora e controla todas as atividades realizadas durante a execução do processo. Por isso, deve ser executada de forma contínua para verificar supervisionar, observar criticamente ou identificar situações que possam impactar mudanças.

Nesta fase os *checklists* são utilizados para realizar a análise crítica com a finalidade de determinar a adequação, suficiência e eficácia do controle de riscos de forma que os objetivos da contratação de TIC sejam alcançados. Na fase 3 são tomadas as medidas de correção que se mostrarem necessárias na revisão do plano de tratamento de riscos, atualização dos registros e documentos gerados, o que garante a que a gestão de riscos esteja sendo efetiva.

Os resultados da fase 3 devem ser registrados na planilha documentadora disponibilizada pela MGR-GRATIC. O link de acesso encontra-se disponível no apêndice H..

A tabela 17 apresenta os procedimentos e práticas a serem adotadas para Monitorar e Controlar Riscos em aquisições de TIC. Além de acompanhar e controlar riscos é preciso que seja realizada a documentação e comunicação dos riscos que ocorrem no decorrer do processo aquisitivo.

Tabela 17 – Fase 3: Monitorar e Controlar Riscos

Objetivo	Revisar e analisar criticamente riscos ocorridos com a finalidade de aprimoramento contínuo da aquisição de TIC.
Entradas	- Plano de Tratamento de Riscos.
Técnicas	- Medição de desempenho. - Reuniões.
Detalhamento da fase	1. Estabelecer indicadores de acompanhamento e controle de riscos: criar checklist contendo atos administrativos e documentos da aquisição de TIC a serem verificados, situação atual, responsável pelo monitoramento, status da publicação, observação e data. O apêndice O apresenta o *checklist* utilizado pela metodologia GRATIC. 2. Acompanhar e controlar a evolução dos riscos. 3. Realizar análise crítica da evolução de riscos. O apêndice P apresenta o painel de indicadores de riscos no processo de aquisição. 4. Divulgar o monitoramento e controle de riscos (Relatório Evolutivo de Riscos).
Responsável	Integrante Técnico Integrante Administrativo
Saídas	- Checklist de riscos. - Painel de indicadores de riscos. - Painel evolutivo de riscos. - Relatório evolutivo de riscos.

Práticas recomendadas:
1. Definir um portfólio de gerenciamento de riscos (COBIT, 2013).
2. Estabelecer indicadores de acompanhamento da implementação de controles de riscos (MPOG, 2017b).
3. Utilizar *checklists*, gráficos e relatórios sumarizados sobre riscos recorrentes (IBGC, 2017).
4. Utilizar o mapa de riscos como ferramenta para monitoramento (MPOG, 2017b).
5. Construir uma planilha de apoio ao processo de gerenciamento de riscos (CGU, 2018).
6. Criar relatórios dos planos de implementação dos controles (MPOG, 2017b).
7. Construir painel de gestão de riscos (CGU, 2018c).
8. Realizar comparação da gestão de riscos com bases normativas, *frameworks*, contextos de governo, percepção de servidores, entre outros (CGU, 2018).
9. Preparar de relatórios periódicos de riscos e controles e opcionalmente indicar a adoção de indicadores-chave de riscos construídos a partir de intervalos de tolerância à perda (IBGC, 2017).
10. Elaborar de uma base de conhecimento de perdas relacionadas aos negócios de forma a auxiliar no direcionamento das decisões relacionadas aos riscos (IBGC, 2017).
11. Apresentar resultados do monitoramento de riscos em reuniões periódicas de planejamento da aquisição de TIC.
12. Realizar reuniões de revisão dos componentes de monitoramento e controle (PMI, 2013 e 2017), (CGU, 2018).
13. Os riscos devem monitorados pelo gestor de riscos (TCU, 2018b).
14. Monitorar e controlar o trabalho do projeto (PMI, 2013 e 2017).
15. Elaborar relatório de desempenho do trabalho (PMI, 2013 e 2017).
16. Realizar auditoria de riscos visando reavaliar riscos (PMI, 2013 e 2017).

Fase 4. Documentar e Comunicar Riscos: consiste em registrar e relatar riscos que ocorrem durante o processo de aquisição de TIC. Nesta fase, além de

documentar e informar riscos e as ações de prevenção ou mitigação contidas no plano de tratamento de riscos, são registradas as lições aprendidas.

Segundo a norma ISO 31000 (2009) a fase de documentação e comunicação é constituída por um processo contínuo e iterativo que uma organização realiza para fornecer, compartilhar ou obter informações necessárias para dialogar com as partes interessadas relacionadas com a gestão de riscos.

Para o COSO (2007) as informações pertinentes à gestão de riscos devem ser identificadas, coletadas e comunicadas de forma coerente e no prazo, a fim de permitir que as pessoas cumpram as suas responsabilidades. Para este *framework* a comunicação pode ser realizada sob a forma de manuais, políticas, memorandos, mensagens de correio eletrônico, notificações em quadros de avisos, mensagens pela Internet e mensagens gravadas em vídeo.

Para a ISO 31000 (2018) convém que a organização estabeleça uma abordagem aprovada para comunicação e consulta para apoiar a estrutura e facilitar a aplicação eficaz da gestão de riscos. A comunicação envolve compartilhar informação com o público-alvo (partes interessadas no processo de aquisição de TIC).O TCU recomenda que seja desenvolvido um plano de comunicação e consulta interna e externa para apoiar esta atividade, seja por meio de um documento formal ou de uma lista de verificação (TCU, 2018).

Na MGR-GRATIC a comunicação de risco é parte integrante do processo de gerenciamento de risco responsável de integrar e informar aos *Stakeholders*, maneiras e procedimentos de como devem agir perante ameaças, evitando que se manifestem e se tornem crises. Nesta metodologia o registro e relato sobre riscos permeia todas as fases da aquisição de TIC, auxiliando a compreensão da gestão sobre a exposição real ao risco relacionado a aquisição de TIC, permitindo a definição de respostas adequadas e informadas sobre os riscos.

Para que a gestão de riscos seja realizada de forma ágil, a MGR-GRATIC disponibiliza um inventário contendo todos os riscos já ocorridos em processos anteriores bem como as ações realizadas para mitigação. A figura 35 apresenta as atividades que compõem a fase 4.

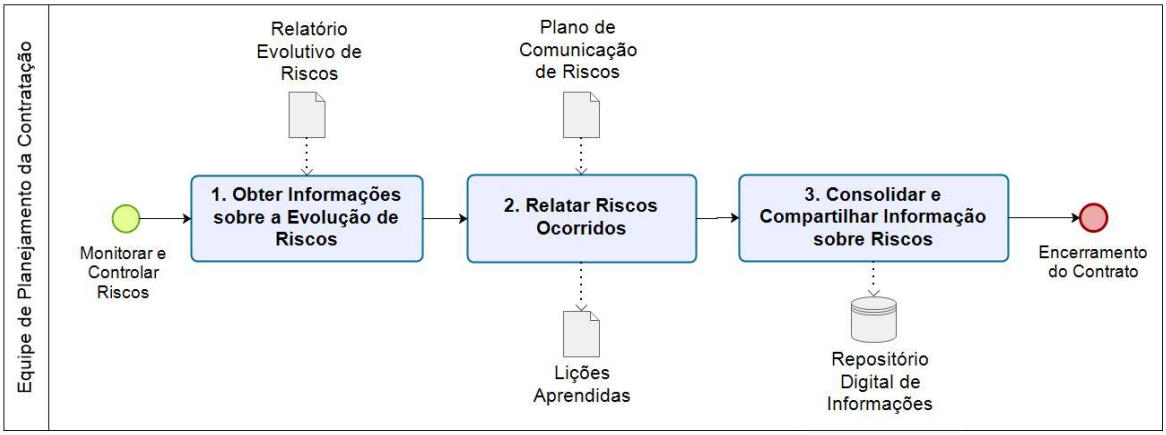


Figura 35 – Fase 4: Documentar e Comunicar Riscos

A figura 35 detalha as 3 atividades da fase 4 da MGR-GRATIC. São elas: obter informações sobre a evolução de riscos, relatar riscos ocorridos e consolidar e compartilhar informação sobre riscos. Esta fase inicia com a obtenção de informações sobre a evolução de riscos através do relatório evolutivo de riscos construído a partir da execução da fase 3 “Monitorar e Controlar Riscos” e encerra com consolidação e compartilhamento de informações sobre riscos através do repositório digital de informações e encerramento do contrato.

A fase 4 descrita na tabela 18 apresenta os procedimentos e boas práticas a serem adotados para registro e relato de riscos durante a execução do contrato. A fase de documentação e comunicação de sobre riscos são realizadas do início ao fim da execução do processo de aquisição de TIC.

Tabela 18 – Fase 4: Documentar e Comunicar Riscos

Objetivo	Registrar e informar os riscos ocorridos durante o processo de aquisição de TIC.
Entradas	- Plano de comunicação de riscos. - Relatório evolutivo de riscos.
Detalhamento do Processo	1. Obter informações sobre a evolução de riscos: risco ocorrido, responsável pela correção, frequência, informar se houve mudanças no processo, ações corretivas realizadas, lições aprendidas e data do registro (apêndice P). 2. Relatar riscos ocorridos: realizar a comunicação das informações produzidas ao longo da execução da gestão de riscos para cada encerramento da fase de aquisição de TIC (ISACA, 2013), (OGC, 2010), (MPOG, 2016) e (TCU, 2018). 3. Consolidar e compartilhar informação sobre riscos: compartilhar aprendizado sobre a gestão de riscos por meio das lições aprendidas durante o processo de aquisição de TIC (base de conhecimento sobre riscos).
Responsável	Equipe de Planejamento da Contratação
Saídas	- Lições aprendidas. - Repositório digital de informações.

Práticas recomendadas:
1. Definir o plano de gerenciamento do projeto (linha de base ou situação atual das áreas afetadas pelo risco incluindo escopo, cronograma e custo (PMI, 2013 e 2017).
2. Definir fontes de dados que possam ser utilizadas para realizar a gestão de riscos (PMI, 2013 e 2017).
3. Definir um plano de comunicação do risco que traz o mapeamento de todos os envolvidos na análise de riscos, estabelece quais as responsabilidades de cada um e define pontos relacionados a comunicação (COBIT, 2013), (OGC, 2010), (MPOG, 2016) e (TCU, 2018).
4. Definir o meio de comunicação sobre os riscos de acordo com os níveis de relacionamento estabelecido no modelo de relacionamento envolvendo os níveis estratégico, tático e operacional (MPOG, 2017b).
5. Desenvolver um relatório a cada seis meses para as partes interessadas (MPOG, 2017b).
6. Preparar relatórios periódicos de riscos e controles e opcionalmente indicar a adoção de indicadores-chave de riscos construídos a partir de intervalos de tolerância à perda (MPOG, 2017b).
7. Elaborar uma base de conhecimento de perdas relacionadas aos negócios de forma a auxiliar no direcionamento das decisões relacionadas aos riscos (MPOG, 2017b).
8. Utilizar a matriz RACI como documento de comunicação sobre riscos durante a execução das fases do processo de gerenciamento de riscos (CGU, 2018) (BERMEJO, 2019).
9. Realizar reuniões de acompanhamento do processo de aquisição (PMI, 2013 e 2017).
10. Definir papéis e responsabilidades para a comunicação de riscos (PMI, 2013 e 2017).
11. Registrar lições aprendidas (PMI, 2013 e 2017).

5.2.2 Técnicas e Ferramentas

Durante as fases do processo de gestão de riscos em aquisições de TIC, a equipe da planejamento da aquisição utiliza diversas técnicas e ferramentas para coleta, análise, avaliação e uso de informações. Elas são recomendadas por normas e metodologias de gestão de riscos, como por exemplo ISO 31010 (2019) e *The*

Orange Book (2019) e pelo *Institute Risk Management (2002)*, PMI (2013; 2017), MGR-GIRC (2017b), MGR-CGU (2018).

a) Técnicas

As técnicas para identificação, análise e avaliação de riscos utilizadas pela MGR-GRATIC são:

- ***Brainstorming*:** recomendada para identificar e avaliar riscos em aquisições de TIC para capturar o maior número de riscos com a participação de todos os integrantes da equipe de planejamento da contratação e equipe de apoio. Esta técnica é indicada para obtenção de uma lista completa de riscos (inventário de riscos) a partir de reuniões em grupo. Ela é recomendada por IRM (2002) e ISO 31010 (ISO, 2019) e utilizada por MGR-GIRC (2017b), MGR-CGU (2018), MGR-TCU (2018b) e MGR-ForRisco (BERMEJO, 2019).
- **Entrevista Estruturada e Semiestruturada:** utilizada para coletar riscos na fase de identificar e avaliar riscos em aquisições de TIC. Esta técnica é sugerida pela ISO 31010 (ISO, 2019) e *The Orange Book* (HMG, 2019) e usada por MGR-TCU (TCU, 2018b).
- **Lista de Verificação (*Checklist*):** desenvolvida com base em informações históricas e conhecimento acumulado. Deve ser revisada periodicamente a partir de reuniões de planejamento da aquisição. Os *checklists* são utilizados para monitoramento e controle de riscos na fase monitorar e controlar riscos em aquisições de TIC. A técnica é indicada pelo *The Orange Book* (HMG, 2019), ISO 31010 (ISO, 2019) e utilizada por MGR-GIRC (2017b) e MGR-CGU (2018).
- **Questionários:** instrumento de coleta de informação composto por questões apresentadas que tem por objetivo propiciar determinado conhecimento sobre gestão de riscos em aquisições de TIC. Questionários são utilizados nas fases de identificar e avaliar riscos, monitorar e controlar riscos. São adotados por (IRM, 2002), (HMG, 2019) e usados por metodologias MGR-GIRC (2017b) e MGR-CGU (2018).
- **Opinião Especializada:** os riscos são identificados por especialistas com experiência relevante em projetos ou áreas de negócios semelhantes. Esses especialistas devem ser identificados pelo gerente do projeto e convidados a

considerar todos os aspectos do projeto, além de sugerir os riscos possíveis com base na sua experiência anterior e nas áreas de especialização. É recomendada por (PMI, 2013;2017) e utilizada por MGR-GRATIC.

b) Ferramentas

As ferramentas de gestão de riscos são utilizadas pela MGR-GRATIC para identificar, avaliar, tratar, monitorar, documentar e comunicar riscos envolvendo o processo de aquisição de TIC. Existem várias ferramentas recomendadas para a gestão de riscos. Neste estudo serão apresentadas apenas as ferramentas utilizadas pela MGR-GRATIC.

- **5W2H:** utilizada na construção do plano de ação na fase para tratar riscos e documentar e comunicar riscos em aquisições de TIC. Ela parte de um evento de risco para organizar as ações e determinar o que será feito para mitigá-lo, por qual razão, por quem, como, quando e onde será feito, além de estimar quanto isso custará. Esta ferramenta é usada para garantir que o planejamento aborde os principais aspectos relativos à ação de controle e comunicação do risco na aquisição de TIC. A figura 36 apresenta uma ação do plano de tratamento de riscos em aquisições de TIC.

Figura 36 - Ferramenta 5W2H

A figura 36 apresenta um exemplo de uma ação existente no plano de tratamento de riscos envolvendo o processo de aquisições de TIC. Como pode ser verificado esta ferramenta pode ser considerada um *checklist* de atividades, prazos e responsabilidades que devem ser desenvolvidos por todos os envolvidos no processo de aquisição de TIC. O apêndice S apresenta o plano de comunicação baseado nesta ferramenta.

- **Gráficos:** representações visuais utilizadas para exibir dados sobre riscos em aquisições de TIC, sejam eles, risco, informação, ou valores numéricos. Na MGR-GRATIC os gráficos são utilizados para demonstrar padrões, tendências e ainda, comparar informações quantitativas num determinado espaço de tempo. O apêndice Q apresenta o painel de indicadores utilizando gráficos. Esta ferramenta é usada pela MGR-ForRisco (BERMEJO, 2019).
- **Planilhas:** avalia os riscos de acordo com os critérios ou parâmetros fornecidos pelos especialistas, técnicos ou responsáveis pela identificação do risco em aquisições de TIC. Na MGR-GRATIC planilhas são utilizadas para classificar riscos, fontes de riscos ou tratamento de riscos com base no nível de risco da aquisição de TIC. O apêndice J apresenta um exemplo de planilha utilizado pela MGR-GRATIC. Esta ferramenta é usada pela MGR-TCU (TCU, 2018b).

- **Relatórios:** conjunto de informações utilizadas para relatar e reportar a evolução dos riscos no decorrer de um determinado espaço de tempo na aquisição de TIC. A MGR-GRATIC apresenta o relatório evolutivo de riscos relacionados a aquisição de TIC no apêndice P. Esta ferramenta é usada nas metodologias MGR-IBGC (IBGC, 2017) e MGR-ForRisco (BERMEJO, 2019).

- **Mapa de Risco:** é uma representação gráfica dos riscos com os níveis de criticidade para o processo de aquisição de TIC. Na MGR-GRATIC o mapa de risco é utilizado para representar a probabilidade e impacto de determinados riscos para o processo de aquisição de TIC. O apêndice M apresenta o mapa de risco usado pela MGR-GRATIC. Esta ferramenta é usada nas metodologias MGR-SISP (MPOG, 2016), MGR-GIRC (MPOG, 2017b), MGR-IBGC (IBGC, 2017), MGR-TCU (TCU, 2018b) e MGR-ForRisco (BERMEJO, 2019).

- **Plano:** utilizado para planejar o tratamento de risco e a comunicação durante a execução das fases de gestão de riscos em aquisições de TIC. Esta ferramenta é adotada pela metodologia MGR-GIRC (MPOG, 2017b), MGR-CGU (CGU, 2018) e recomendada pelo *The Orange Book (*OCG, 2010).

5.2.3 Artefatos

Os artefatos utilizados pela metodologia GRATIC são documentos utilizados para realização da gestão de riscos de forma estruturada e transparente. Nesta metodologia foram definidos dois artefatos: planilha documentadora (mapa de gerenciamento de riscos) e repositório digital de informações.

a) Planilha Documentadora: utilizada para registro e relato de todas as atividades realizadas nas fases da metodologia de gestão de riscos em aquisições de TIC. Na MGR-GRATIC recebe o nome de mapa de gerenciamento de riscos. O endereço eletrônico para acesso a planilha documentadora encontra-se disponível no apêndice H. Este artefato é semelhante ao disponibilizado pela metodologia MGR-GIRC (2017b).

- **Inventário de Riscos:** lista contendo os riscos que comprometem o cumprimento dos objetivos organizacionais. Na MGR-GRATIC esta lista contém os campos: nº, descrição do risco, proprietário do risco, causa do riscos, efeito/dano/consequência, categoria e fase da contratação. O apêndice J apresenta o inventário de riscos contendo dados utilizados no estudo de caso.
- **Matriz de Probabilidade x Impacto:** mapa que permite de forma visual identificar quais são os riscos que devem receber mais atenção. Na MGR-GRATIC é utilizada para avaliação de riscos do processo de aquisição de TIC. O apêndice M apresenta a matriz construída no estudo de caso.
- **Plano de Tratamento de Riscos:** consiste em definir respostas a riscos identificados e avaliados durante a execução do processo de aquisição de TIC. Na MGR-GRATIC o plano de tratamento de riscos é construído a partir da ferramenta 5W2H e está demonstrado no apêndice N.

- **Painel de Riscos Recorrentes:** apresenta os riscos ocorridos durante a aquisição de TIC. Na MGR-GRATIC é utilizado para apresentar de forma clara e objetiva os riscos que ocorreram durante o processo de aquisição de TIC. O apêndice R apresenta o painel de riscos recorrentes relacionados estudo de caso realizado.
- **Relatório Evolutivo de Riscos:** mostra a evolução do processo de identificação, análise de riscos, tratamento, monitoramento e controle de riscos na aquisição de TIC. Na MGR-GRATIC apresenta os riscos ocorridos durante as fases do processo de aquisição, as ações corretivas realizadas e lições aprendidas, conforme mostra o apêndice P.
- **Painel de Indicadores de Riscos:** relatório sumarizado sobre a aquisição de TIC. Apresenta o quantitativo de eventos que geraram ameaças para a execução do processo de aquisição de TIC. Na MGR-GRATIC é utilizado para apresentar de forma gráfica os riscos ocorridos durante o processo de aquisição de TIC. O apêndice Q apresenta o painel de indicadores de riscos de um processo de aquisição realizado no estudo de caso.
- **Plano de Comunicação:** registra as estratégias de comunicação a serem adotadas durante a execução da gestão de riscos em aquisições de TIC. A MGR-GRATIC usa a ferramenta 5W2H para sua construção. O apêndice S apresenta o plano de comunicação utilizado no estudo de caso.

b) Repositório Digital de Informações: local utilizado para compartilhamento de lições aprendidas durante a gestão de riscos em aquisições de TIC. No repositório digital de Informações da MGR-GRATIC estão disponibilizados o mapa de gerenciamento de riscos, o manual de utilização da metodologia e materiais de referência sobre gestão de riscos. O apêndice H apresenta o endereço eletrônico para acesso ao repositório digital de informações GRATIC.

6 DEMONSTRAÇÃO E AVALIAÇÃO

O capítulo apresenta os resultados obtidos em relação ao uso da solução proposta nesta dissertação em um contexto real. Para demonstrar e avaliar a solução para o problema relatado no capítulo 4 foi adotado o uso de estudo de caso exploratório único. Inicialmente descreve o contexto da instituição escolhida e os sujeitos da pesquisa. Em seguida apresenta a solução, o seu uso e avaliação. Por fim, detalha os resultados obtidos, as contribuições dos especialistas e finaliza com a avaliação crítica realizada pela pesquisadora.

6.1 ESTUDO DE CASO

O estudo de caso adotado nesta pesquisa visa avaliar o uso da MGR-GRATIC em um contexto real. Neste sentido, para realizar a avaliação foram definidas algumas etapas a serem cumpridas, são elas: definição do contexto da instituição, público-alvo, apresentação da solução, uso, avaliação e resultados obtidos, contribuições dos especialistas na área e visão crítica da solução.

O estudo de caso foi realizado entre os meses de setembro a novembro de 2019. Neste estudo, a pesquisadora tem o papel de construtora e observadora do uso dos artefatos propostos pela MGR-GRATIC.

6.1.1 Contexto da Instituição

O Instituto Federal de Educação escolhido para a realização do estudo de caso está localizado na região norte do Brasil. Esta instituição de ensino foi escolhida levando em consideração a facilidade de acesso às informações e disponibilidade dos especialistas em aquisições de TIC para testar e avaliar os artefatos propostos pela solução, bem como as dificuldades que tem enfrentado atualmente em relação a gerir riscos em aquisições de TIC.

A instituição de ensino escolhida tem experiência em elaborar contratações de grande porte e possui significativo orçamento para aquisições de TIC no âmbito do governo federal. Entretanto, a gestão de riscos ainda não é realizada conforme

as boas práticas recomendadas pela legislação vigente. Ela aceitou fazer parte do estudo do caso, em razão de buscar melhorias que maximizam o conhecimento organizacional neste processo, uma vez que têm enfrentado nos últimos anos vários desafios relacionados a gestão de riscos nas aquisições de TIC.

Optou-se por preservar a identidade desta instituição pública de forma a manter a privacidade das informações institucionais e não expor seus problemas, fragilidades e riscos. Por este motivo, será referenciada neste estudo como “Instituto Federal de Educação do Norte”.

6.1.2 Sujeitos de Pesquisa

O público-alvo para realização do estudo de caso são 8 servidores públicos que trabalham com o processo de aquisição de TIC no Instituto Federal de Educação da região norte, seja realizando o papel de requisitante da solução, gestor do contrato, fiscal do contrato, integrante administrativo ou integrante técnico, executando atividades de análise de riscos, avaliação de propostas, respostas aos esclarecimentos e impugnações, gestão e fiscalização de contratos. Estes servidores são especialistas na área de TIC e possuem vários anos de experiência em aquisições de TIC. Os perfis dos participantes deste estudo de caso estão disponibilizados no apêndice F.

Para escolher quais servidores públicos participariam do estudo de caso levou-se em consideração a definição dos atores existente no modelo de contratação de TIC apresentado no guia de boas práticas em contratações de TIC do MPOG (2018) e na Instrução Normativa ME/SGD Nº 1/2019 (Brasil, 2019b). Os servidores participantes do estudo de caso fazem parte da atual equipe de planejamento de aquisições de TIC e aceitaram espontaneamente participar da pesquisa.

6.1.3 Apresentação da Solução

A solução para gestão de riscos em aquisições de TIC foi apresentada em uma reunião com servidores previamente convidados para participar da pesquisa no dia 2 de setembro de 2019. A solução foi demonstrada através do manual da MGR-GRATIC e o preenchimento do mapa de gerenciamento de riscos. Posteriormente foram disponibilizados para todos os participantes do estudo de caso, os documentos referentes a metodologia de gestão de riscos através do repositório digital de informações.

Na ocasião, alguns participantes do estudo de caso perguntaram sobre os critérios de definição dos riscos e qual processo de aquisição deveriam usar. Foi informado que a equipe deveria utilizar os critérios definidos na MGR-GRATIC e os participantes do estudo de caso poderiam escolher quais processos seriam utilizados para avaliar a solução proposta.

A equipe de planejamento da aquisição definiu que seriam dois processos aquisitivos. O primeiro seria sobre aquisição de equipamentos de informática e o segundo deveria ser sobre contratação de empresa especializada em prestação de serviços de link para acesso à internet, processos comuns, relativamente simples e realizados por todas instituições públicas brasileiras.

6.1.4 Uso da Solução

A estratégia adotada para o uso da solução, acordada com os participantes do estudo de caso é que o preenchimento da planilha documentadora fosse realizado de forma centralizada, ou seja, um único documento deveria ser preenchido por todos, de forma a permitir o aprendizado organizacional coletivo e participativo. Foi definido entre os membros da equipe de planejamento da contratação que a metodologia seria aplicada em dois momentos: o primeiro seria realizado entre os dias 09/09/2019 a 20/09/2019 utilizando o processo de aquisição de equipamentos de TIC que já tinha ocorrido, ou seja foi selecionado um processo *post mortem (já ocorrido)*.

Entre os dias 23/09/2019 a 27/09/2019 foram reservados para ajustes na MGR-GRATIC e mapa de gerenciamento de riscos. O segundo momento foi realizado entre os dias 30/09/2019 a 11/10/2019 para a contratação de empresa especializada em prestação de serviços de link para acesso à Internet.

Entre os dias 23 a 27 de setembro de 2019 foram realizadas alterações no artefato planilha documentadora, no que refere-se à definição de pesos para cálculo de probabilidade e impacto, correções e atualizações dos riscos já identificados no inventário de riscos, ajustes na fórmula para cálculo e definição de nível de impacto, correção na fórmula para classificação de probabilidade e acréscimo de indicadores de desempenho na planilha "painel de indicadores". No artefato repositório digital de informações foram acrescentados materiais de referência sugeridos pelos participantes do estudo de caso e inserida a nova planilha documentadora atualizada após a execução do primeiro momento.

Na medida que os participantes do estudo de caso tinham dúvidas sobre o preenchimento do mapa de gerenciamento de riscos, a pesquisadora explicava as fases que compõem a metodologia de gestão de riscos e como a planilha documentadora deveria ser utilizada. Tendo em vista que a MGR-GRATIC tem manual de utilização, cujo endereço eletrônico encontra-se disponibilizado através do apêndice H, poucas dúvidas surgiram.

a) Primeiro momento - aquisição de equipamentos de TIC **(09/09/2019 – 20/09/2019):** neste momento, ao iniciar a execução da MGR-GRATIC os participantes do estudo de caso tiveram dúvidas em relação a definição de categorias de riscos e o cálculo da probabilidade e impacto. Neste sentido, a solução proposta apresentou necessidades de detalhamento das fases e cálculos de probabilidade e impacto.

Os participantes do estudo de caso sugeriram melhorias na definição do registro de atividades de forma a tornar as fases da MGR-GRATIC mais estruturadas e organizadas, principalmente na fase de identificar e avaliar riscos em aquisições de TIC. Eles recomendaram reestruturar a fase de identificar e avaliar riscos de forma que os campos na medida do possível sejam previamente preenchidos o que pode facilitar o trabalho da equipe de planejamento da contratação.

Os membros da equipe de planejamento da contratação do Instituto Federal de Educação da região norte sugeriram também a inserção de novos riscos e alterações nos pesos para cálculo de probabilidade e impacto dos riscos nas aquisições de TIC. Estas sugestões foram avaliadas pela pesquisadora e as alterações foram feitas antes do início do segundo momento.

Para o segundo momento (prestação de serviços de *link* para acesso à Internet) foram realizadas adequações em todas as fases existentes na planilha documentadora, disponibilizada no apêndice H, de forma que a equipe de planejamento da contratação realizasse apenas a inserção de novos riscos, conferência e atualização das informações existentes. O segundo momento foi feito utilizando uma versão atualizada do mapa de gerenciamento de riscos.

b) Segundo momento – contratação de empresa especializada em prestação de serviços de *link* para acesso à Internet **(30/09/2019 – 11/10/2019):** em razão dos participantes do estudo de caso já terem utilizado o mapa de gerenciamento de riscos no primeiro momento, o preenchimento da planilha documentadora no segundo momento foi de certa forma mais rápido. Os participantes do estudo de caso informaram que nem sempre os riscos de uma aquisição de TIC se repete em outra aquisição, ou seja podem ser diferentes.

Este fato ocorreu no segundo momento, pois prestação de serviços tem características e cláusulas contratuais diferente de equipamentos de TIC, assim como também acordos de níveis de serviços, cláusulas sobre vínculo empregatício, formas de prestação de serviços e pagamento. Os membros da equipe de planejamento da contratação identificaram riscos que são específicos para prestação de serviços e que não foram reportados no primeiro momento. São eles: rompimento do contrato em razão de prestação de serviços com baixa qualidade técnica, interrupção da prestação de serviços por erros técnicos, política econômica obrigando repactuação contratual.

6.1.5 Resultados Obtidos a partir do uso da Solução

Os resultados obtidos com o uso da MGR-GRATIC nos dois processos de aquisição de TIC foram satisfatórios apresentando redução na incidência de riscos que são recorrentes em todas as aquisições de TIC, como por exemplo: inconsistências nas especificações técnicas do termo de referência, inserção de itens que geram excessos de questionamentos e impugnações. Antes do uso da solução ocorriam riscos relacionados a pesquisa de mercado, estudo de viabilidade da solução escolhida, falhas nas especificações do objeto, divergências entre o termo de referência e o edital de licitação.

Em processos realizados em anos anteriores ocorriam muitos questionamentos e impugnações por falta de comunicação entre a equipe de planejamento da contratação e a equipe de apoio. Com o uso da MGR-GRATIC a incidência média de 20 riscos ocorridos baixou para 9. Verificou-se que a medida que a MGR-GRATIC era utilizada pela equipe de planejamento da contratação e apoio, os controles foram aperfeiçoados, de forma que os riscos foram mitigados não ocasionando impactos negativos significativos para a instituição.

Com o uso da solução foi verificado a necessidade de se ter várias versões do mapa de gerenciamento de riscos de forma a atender as especificidades de cada tipo de aquisição de TIC. Neste sentido, devem ser criadas planilhas para aquisição de equipamentos de TIC, prestação de serviços, compra de suprimentos de TIC e adesão a registro de preços.

Portanto, a MGR-GRATIC além de realizar o monitoramento e o controle de riscos, documenta todas as fases de gestão de riscos, o que facilita o processo de decisão em relação a qual ação deve ser realizada para mitigar riscos, como por exemplo: corrigir inconsistências no termo de referência e no Edital, realizar novamente a pesquisa de mercado e estudo técnico preliminar de forma a evitar licitações fracassadas ou desertas, direcionamento de marca ou modelo entre outros riscos. A tabela 19 apresenta informações obtidas a partir do uso da MGR-GRATIC.

Tabela 19 – Resultados Obtidos com o Uso da MGR-GRATIC

Riscos ocorridos nos dois momentos de uso da MGR-GRATIC	Aquisição de TIC	
	Equipamentos de TIC	Prestação de Serviço
Questionamentos	4	3
Impugnações	3	2
Riscos identificados	63	87
Riscos ocorridos	9	7
Riscos mitigados	9	7
Correção de Termo de Referência	4	2
Correção de Edital	4	3

A tabela 19 mostra os resultados obtidos após o uso da MGR-GRATIC. Ela sintetiza o quantitativo de riscos identificados nos dois momentos em que a solução foi avaliada, segundo a opinião dos participantes deste estudo de caso.

A solução foi avaliada no segundo momento de forma prática em um contexto real por meio de um processo de contratação de empresa especializada em prestação de serviços de acesso à internet que ocorria naquele momento. Naquela ocasião foi possível observar a importância do monitoramento e controle de riscos nas fases do processo de aquisição de TIC.

Ao utilizar a solução proposta neste estudo observou-se que a medida que a equipe de planejamento e apoio usava a planilha documentadora para gerenciar riscos em aquisições de TIC, mais riscos eram identificados e mitigados. Este fato deverá ocorrer sempre, pois cada processo aquisitivo realizado na maioria das vezes é executado por uma equipe de planejamento da contratação diferente. Ao realizar a gestão de riscos em aquisições de TIC deve ser considerada a capacidade e habilidade técnica da equipe de planejamento da aquisição, o contexto interno e externo da organização, bem como a política e a economia do país.

Os participantes do estudo de caso relataram a importância da MGR-GRATIC para o contexto utilizado, uma vez que foi possível observar na prática o quanto a gestão de riscos se torna eficiente através da estruturação, documentação, monitoramento e controle de riscos. Neste sentido, a solução se mostrou útil no âmbito das instituições públicas brasileiras.

Vale ressaltar, segundo a opinião dos participantes do estudo de caso, que o fato dos resultados serem diferentes pode ser em razão de serem processos com

características e particularidades específicas exigindo o conhecimento técnico e habilidade da equipe de planejamento na gestão de riscos em todas as fases da contratação. Ressalta-se também, que um participante considera que a gestão de riscos no processo de aquisição de TIC é irrelevante não necessitando de monitoramento e controle específicos.

Na opinião de um avaliador, a partir do uso da solução proposta neste estudo "*foi possível acompanhar a execução de todas as fases do processo de aquisição de TIC*". Outro avaliador considerou "*interessante a identificação de riscos apresentada no inventário de riscos tornando o processo mais ágil*". Vale observar também que um avaliador considera mais interessante o "*uso de um software específico para a aplicação da MGR-GRATIC*".

De forma a compreender quais são os riscos recorrentes em todo o processo de aquisição de TIC os participantes do estudo de caso construíram uma lista contendo os riscos dividida por fases do processo de aquisição. Inicialmente a planilha documentadora continha os riscos e controles mapeados pelo TCU em 2013 e outros riscos identificados na *grey literature*. Em seguida, foram acrescentadas as sugestões feitas pelos colaboradores desta pesquisa.

Conforme a equipe de planejamento da contratação utilizava a planilha documentadora nos processos avaliados no estudo de caso, diversos riscos foram acrescentados ou atualizados. Após a finalização dos dois momentos de avaliação da solução os participantes do estudo de caso em uma reunião através de grupo focal, mapearam e categorizaram os riscos em cada fase do processo de aquisição. A figura 37 apresenta alguns dos riscos comuns aos processos de aquisição de TIC categorizados nas fases de planejamento da contratação, seleção do fornecedor e gestão do contrato.

Figura 37 – Riscos Recorrentes em Aquisições de TIC

Os riscos apresentados na figura 37 aparecem nas duas planilhas documentadoras utilizadas para avaliação da MGR-GRATIC. Estes riscos foram gerenciados através do inventário de riscos, mapa de probabilidade x impacto, *checklist* de monitoramento e acompanhamento das fases de aquisição de TIC, relatório evolutivo de riscos e painel de indicadores. Segundo os participantes do estudo de caso, grande parte dos riscos ocorridos no processo de aquisição de TIC referem-se a erros e omissões por parte dos diversos atores envolvidos na execução do processo licitatório.

6.1.6 Avaliação do uso da Solução

A avaliação da solução foi realizada pelos participantes do estudo de caso. Estes servidores fazem parte da atual equipe de planejamento da aquisição do Instituto Federal de Educação do Norte, instituição utilizada no estudo de caso.

Oito servidores públicos foram convidados a participaram da avaliação do uso da solução. Esta avaliação foi realizada em uma reunião no dia 14/11/2019. Na ocasião foram apresentados os resultados obtidos com o uso da MGR-GRATIC.

Os participantes do estudo de caso relataram a experiência obtida com o uso da solução e puderam expressar suas opiniões. Neste momento, sugeriram melhorias para os trabalhos futuros, bem como validaram através de *brainstorming* os riscos recorrentes em toda aquisição de TIC.

Após o uso de *brainstorming* foi solicitado aos participantes do estudo de caso que realizassem a avaliação da MGR-GRATIC. Para isso, a pesquisadora entregou um questionário contendo o roteiro sobre a avaliação da solução disponibilizado no apêndice G.

A avaliação do uso da solução contemplou os dois processos de aquisição de TIC utilizados pela equipe de planejamento da contratação. O roteiro proposto para a avaliação da solução é baseado em Lacerda (2013) apud March e Smith (1995) e tem como finalidade medir o comportamento do artefato para solução do problema e comparar os resultados obtidos com os requisitos previamente definidos em um contexto real, Instituto Federal de Educação da região norte.

O questionário foi construído a partir da escala likert (LIKERT, 1932) utilizando como requisitos de solução: operacionalidade, eficiência, generalidade e facilidade de uso; e como respostas: Concordo Totalmente, Concordo Parcialmente, Indiferente, Discordo Parcialmente e Discordo Totalmente. A tabela 20 apresenta as questões que foram utilizadas para avaliar a MGR-GRATIC. As questões foram adaptadas de March e Smith (1995).

Tabela 20 - Avaliação da Solução

Nº	Descrição	Requisito
1	A solução apresentada é capaz de executar as atividades definidas para realizar a gestão de riscos em aquisições de TIC?	Operacionalidade
2	A solução apresentada contribui para que a gestão de riscos em contratações de TIC seja realizada no tempo previsto?	Eficiência
3	A solução apresentada pode ser utilizada para outro tipo de aquisição?	Generalidade
4	A solução apresentada é de fácil compreensão e uso?	Facilidade de uso

A partir da definição das questões que fazem parte da avaliação da MGR-GRATIC apresentada na tabela 20, foi definida a estratégia de avaliação demonstrada na tabela 21. A estratégia define o que será avaliado?, quem avaliará?, como será avaliado? e quando será avaliado?

Tabela 21 – Estratégia para Avaliação da Solução

O que será avaliado?	Quem avaliará?	Como será avaliado?	Quando será avaliado?
Aprendizagem dos participantes do estudo de caso	Pesquisadora	Por meio de grupo focal de avaliação e feedback.	No início, durante e ao final do estudo de caso.
Metodologia GRATIC	A equipe de planejamento da contratação do IF	Questionário elaborado pela pesquisadora.	No final do estudo de caso.
	Pesquisadora	A partir da análise dos dados coletados.	No final do estudo de caso.

A condução da avaliação proposta na tabela 20 foi importante para aperfeiçoar a solução proposta neste estudo, a partir das sugestões de melhoria feitas pelos participantes do estudo de caso, algumas atividades foram otimizadas e simplificadas como por exemplo a identificação e avaliação de riscos. A avaliação da MGR-GRATIC foi realizada por meio da formação de um grupo focal com os participantes do estudo de caso. A consolidação da avaliação é apresentada na tabela 22.

Tabela 22 – Avaliação do Uso da Solução

Nº	Descrição	Requisito	CT	CP	I	DP	DT
1	A solução apresentada é capaz de executar as atividades definidas para realizar a gestão de riscos em aquisições de TIC?	Operacionalidade	5	0	1	1	1
2	A solução apresentada contribui para que a gestão de riscos em contratações de TIC seja realizada no tempo previsto?	Eficiência	4	1	1	1	1
3	A solução apresentada pode ser utilizada para outro tipo de aquisição?	Generalidade	4	0	1	1	2
4	A solução apresentada é de fácil compreensão e uso?	Facilidade de uso	5	1	0	1	1

Legenda: CT- Concordo Totalmente | CP - Concordo Parcialmente | I - Indiferente | DP - Discordo Parcialmente | DT - Discordo Totalmente

A tabela 22 apresenta os resultados obtidos na avaliação da solução proposta. Em relação à operacionalidade, quando os participantes do estudo de caso foram questionados se a solução apresentada é capaz de executar a tarefa pretendida ou a capacidade das pessoas utilizarem a MGR-GRATIC para gestão de riscos em aquisições de TIC, de 8 participantes do estudo de caso, 5 pessoas consideram que a solução atende o requisito.

Segundo os participantes do estudo de caso, a solução possui plena condição de realizar a gestão de riscos em aquisições de TIC. Para um dos participantes a "*solução contempla todas as atividades necessárias para a realização do controle de riscos, restando apenas acompanhar as constantes mudanças no cenário político e econômico*".

O requisito eficiência mede a capacidade de execução de uma fase de modo correto e no tempo previsto. Segundo os dados apresentados na figura 38, 4 participantes do estudo de caso consideram que a MGR-GRATIC contribui para diminuir o tempo de realização da gestão de riscos em aquisições de TIC, porém 4 pessoas não concordam totalmente.

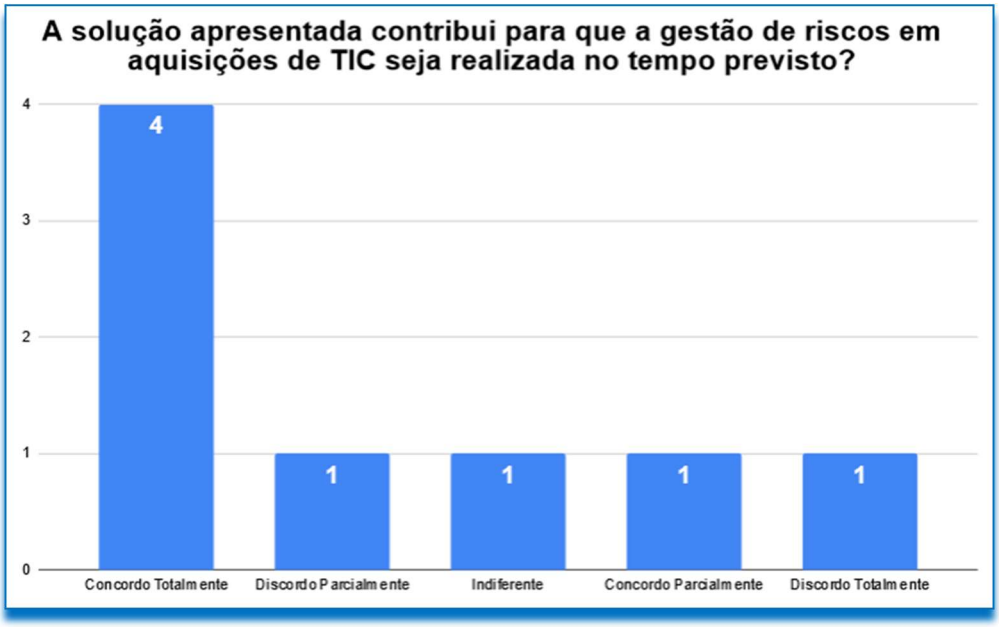


Figura 38 - Avaliação da Eficiência da Solução

Para os participantes do estudo de caso a solução atende o requisito eficiência, conforme mostra a figura 38. Para um dos participantes do estudo de

caso "*a solução proposta pode reduzir o tempo de execução da gestão de riscos no processo licitatório, uma vez que os riscos já estão mapeados no inventário de riscos restando apenas realizar a conferência das informações apresentadas de acordo com o contexto interno e externo da instituição o que pode evitar perda de tempo para executar a fase de identificar a avaliar os riscos*".

Entretanto, é importante ressaltar que na opinião de 4 participantes, a MGR-GRATIC ainda tem que evoluir para que a realização da gestão de riscos seja feita de forma ágil. Vale ressaltar que o processo de aquisição de TIC é influenciado por fatores internos e externos, como por exemplo: a política de cortes orçamentários do governo federal, a falta de repasse de verbas federais exclusivas para a educação por parte de parlamentares estaduais e federais.

Os participantes do estudo de caso consideraram que a solução apresentada é eficiente uma vez que o prazo médio para a realização da análise de riscos antes do uso MGR-GRATIC era de 1 ano, considerando todas as fases do processo de contratação de TIC, questionamentos, impugnações e tipos de contratação. Os membros da equipe de planejamento da contratação destacam que os contratos de prestação de serviços continuados são os processos mais demorados em razão do tempo de duração de contrato, podendo chegar a 60 meses.

Em relação ao requisito generalidade foi avaliado se a solução pode ser utilizada para outro tipo de processo de aquisição. Para 4 dos participantes do estudo de caso o mapa de gerenciamento de riscos pode ser utilizado para outro tipo de aquisição uma vez que as fases definidas na MGR-GRATIC são comuns a todos os modelos e metodologias de gestão de riscos existentes no mercado. Porém sabe-se que o processo de aquisição possui particularidades em cada instituição, por isso os participantes do estudo de caso recomendam realizar adequações.

Segundo um dos participantes do estudo de caso, "*embora a MGR-GRATIC foi construída a partir de boas práticas utilizadas pelo mercado em relação à gestão de riscos, ela não pode ser utilizada para qualquer tipo de aquisição de TIC, uma vez que cada processo licitatório possui suas particularidades e legislação a ser seguida. Neste sentido, o inventário de riscos não é o mesmo para todos os processos de aquisição*". Uma aquisição de equipamentos possui características e

riscos diferentes de uma prestação de serviços. A figura 39 apresenta os resultados obtidos neste requisito.

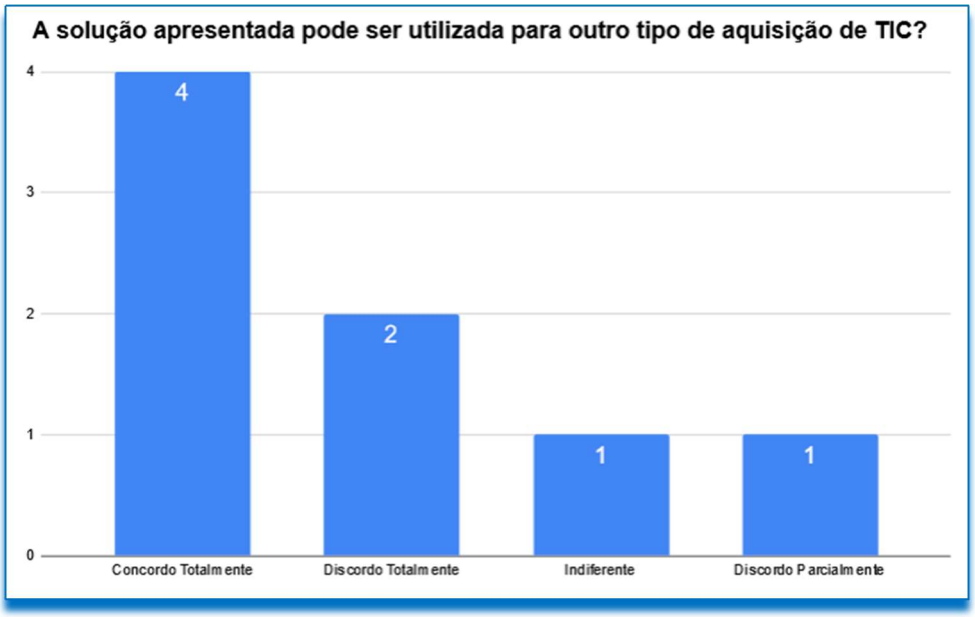


Figura 39 - Avaliação de Generalidade da Solução

Segundo a figura 39, 4 participantes do estudo de caso consideram que a solução pode ser utilizada no processo de aquisição como um todo, bastando apenas algumas adequações no inventário de riscos. Entretanto, vale ressaltar que foi avaliada em apenas um Instituto Federal de Educação, o que pode não corresponder a opinião das demais instituições públicas brasileiras. Para 2 participantes do estudo de caso o mapa de gerenciamento de riscos não pode ser generalizado para outros tipos de aquisição, uma vez que os riscos mudam em razão da descrição do objeto.

Para os participantes do estudo de caso o mapa de gerenciamento de riscos apresentado na solução é de fácil compreensão e uso. Conforme apresenta a figura 40, cinco participantes do estudo de caso conseguiram utilizar a planilha documentadora sem interferência da pesquisadora.

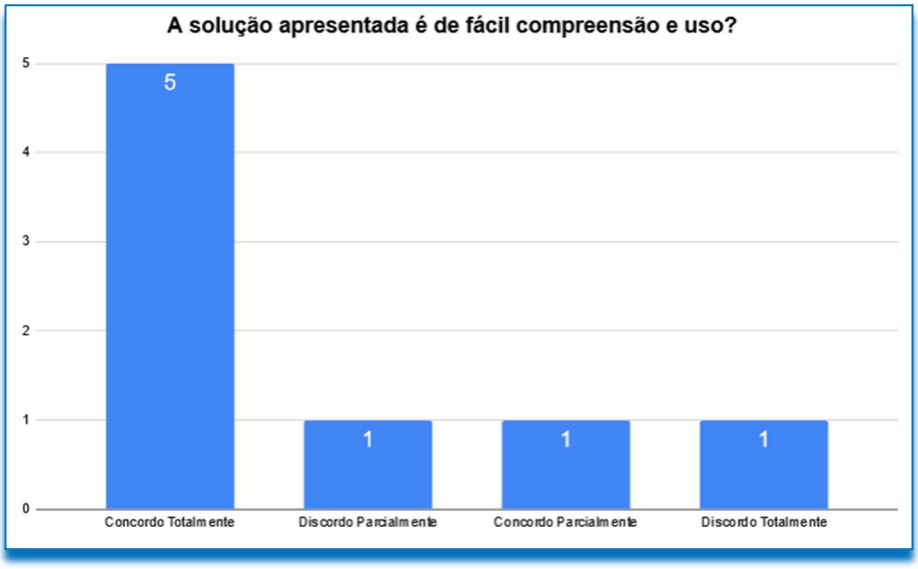


Figura 40 - Avaliação sobre Compreensão e Uso da Solução

De acordo com a figura 40, a maioria dos participantes do estudo de caso consideram que a solução é de fácil entendimento e preenchimento. O mapa de gerenciamento de riscos facilita a execução das fases de gestão de riscos, uma vez que possui o inventário de riscos, restando apenas a conferência dos dados e algumas alterações na seleção de riscos dependendo de cada tipo de aquisição. Dentro desta visão, um dos participantes do estudo de caso sugere o "*uso um software específico no lugar de uma planilha documentadora de forma a tornar a solução mais atrativa e eficiente".*

6.1.7 Contribuições dos Especialistas na área de Aquisições de TIC

No decorrer do estudo de caso alguns participantes fizeram sugestões importantes que devem ser consideradas ao utilizar a MGR-GRATIC para aumentar a eficiência da gestão de riscos em aquisições de TIC. Dentre elas devem ser destacadas:

> "*Para que a gestão de riscos seja realizada através da MGR-GRATIC de forma efetiva no processo de aquisições de TIC, deve ser levado em consideração o planejamento da contratação, o cronograma de trabalho, a distribuição de tarefas e a definição clara e objetiva de papéis e responsabilidades de cada membro da equipe de planejamento e também devem ser realizadas atualizações periódicas dos riscos já identificados bem como as ações corretivas*".

> "*A MGR-GRATIC deve avaliar e monitorar riscos em aquisições de TIC continuamente, através de painéis de riscos e indicadores de desempenho, de forma a ter pontos de controle sobre as incertezas que possam afetar o cumprimento dos objetivos organizacionais envolvendo aquisições de TIC*".
>
> "*A gestão de riscos proposta pela MGR-GRATIC deve ser sistematizada e transparente em todas as fases da contratação. Portanto, é importante que as fases envolvendo a gestão de riscos sejam planejadas, atualizadas continuamente e socializadas em reuniões periódicas*".
>
> "*A MGR-GRATIC deve estabelecer pontos de controle em todas as fases da contratação, de forma a garantir o sucesso do processo licitatório. A verificação pode ser realizada através de checklists, apresentados em reuniões periódicas*".
>
> "Para que a *gestão riscos seja considerada efetiva, deve-se definir uma sequência de fases a serem seguidas e ser realizado o monitoramento e controle de riscos por meio de pontos de controle e indicadores de desempenho atualizados continuamente*."

As contribuições realizadas pelos participantes do estudo de caso serviram para otimização das fases de identificar e avaliar riscos, tratar riscos, monitorar e controlar riscos, documentar e comunicar riscos. Com base na avaliação realizada pelos membros da equipe de planejamento da contratação do Instituto Federal de Educação da região norte, as planilhas contidas no mapa de gerenciamento de riscos foram aperfeiçoadas.

6.1.8 Visão Crítica da Solução

Os resultados da avaliação da solução indicam que a MGR-GRATIC dispõe de informações necessárias para auxiliar a gestão de riscos envolvendo contratações de TIC no âmbito dos Institutos Federais de Educação. Também possui condições para ser utilizada por organizações públicas brasileiras que apresentem dificuldades em monitorar e controlar riscos inerentes ao processo de aquisições de TIC.

A MGR-GRATIC foi construída a partir de abordagens de gestão de riscos que são consideradas como referência no mercado e utiliza as recomendações da legislação vigente sobre aquisições de TIC. Ela enfatiza o monitoramento e controle da gestão de riscos em todas as fases da contratação através de rotinas padronizadas e documentadas envolvendo todo o processo de aquisição de TIC.

A avaliação da MGR-GRATIC mostrou-se viável no âmbito de um instituto federal de educação, os resultados iniciais sugerem que pode ser usada em outras instituições públicas brasileiras. Entretanto, mesmo com o resultado positivo, é necessário executar a metodologia em outros contextos que compõem a Administração Pública, uma vez que cada organização possui suas peculiaridades e realiza a gestão de riscos de forma diferente de acordo com o contexto interno e externo.

Através da análise do resultado da avaliação do uso da MGR-GRATIC verifica-se que a eficiência da gestão de riscos em aquisições de TIC exige um esforço inicial para validar todos os riscos na primeira fase (identificar e avaliar riscos). Esta situação ocorre em razão de que o conhecimento sobre a gestão de riscos depende da experiência dos envolvidos e da necessidade de cada organização bem como de constantes mudanças no cenário organizacional, político e econômico.

Neste sentido, a MGR-GRATIC auxilia os gestores no processo de tomada de decisão em relação aos riscos em aquisições de TIC ao estruturar fases para identificação, avaliação, tratamento, monitoramento, comunicação e aprendizado sobre riscos. No entanto, não resolve problemas relacionados a falta de governança e gestão dentro das instituições públicas brasileiras.

Como a transformação digital é contínua e dinâmica, a evolução e otimização das fases da MGR-GRATIC se fazem necessárias. Embora ela tenha sido construída para se adaptar a mudanças, alguns ajustes sempre são necessários.

A vantagem do uso desta solução em relação as demais metodologias existentes no mercado, deve-se ao fato de dispor de um inventário contendo riscos e controles que permite que a equipe de planejamento da aquisição possa adaptá-lo a sua realidade e necessidade, uma vez que as fases estão previamente definidas e validadas por especialistas em aquisições de TIC. Além deste diferencial possui um repositório digital de informações que pode ser utilizado para compartilhamento do aprendizado corporativo sobre riscos.

7 CONCLUSÕES, LIMITAÇÕES E TRABALHOS FUTUROS

O capítulo aborda a conclusão do estudo. Primeiramente irá apresentar as considerações finais e os trabalhos relacionados com a temática desta pesquisa. Em seguida, detalha as limitações da pesquisa, as contribuições do estudo e perspectivas futuras.

7.1 CONSIDERAÇÕES FINAIS

A gestão de riscos relacionada ao processo de aquisição de TIC dentro das instituições públicas brasileiras tem sido um dos grandes desafios para os gestores, uma vez que os riscos não gerenciados podem impactar o não cumprimento dos objetivos organizacionais. O objetivo geral desta pesquisa foi *propor uma metodologia para gerenciar riscos em aquisições de TIC de forma eficiente no contexto das instituições públicas brasileiras.* Para isso, buscou compreender: *como realizar de forma eficiente a gestão de riscos em aquisições de TIC nas instituições públicas brasileiras?*

Com o propósito de responder este questionamento, foram realizadas pesquisas do tipo documental e bibliográfica, aplicação de questionários e entrevistas com especialistas na área de aquisições de TIC. A partir da compreensão do problema por meio de uma visão prática, uma metodologia para gestão de riscos foi idealizada.

Os resultados obtidos na avaliação com especialistas na área de aquisição de TIC do Instituto Federal de Educação, utilizado como estudo de caso, indicam que a solução proposta se mostra viável do ponto de vista prático. A MGR-GRATIC apresenta um percentual considerável de aceitação por parte dos membros da equipe de planejamento da contratação que participaram do estudo de caso.

A MGR-GRATIC pode ser um instrumento para apoiar a tomada de decisão em relação a ações de monitoramento e controle de riscos no processo de aquisições de TIC. Ficou evidenciado que as instituições públicas brasileiras podem melhorar seu controle de riscos utilizando uma sequência de fases para

identificação, análise, avaliação, tratamento, monitoramento, informação e aprendizado sobre riscos envolvendo o processo de aquisição de TIC.

Nesta pesquisa quatro aspectos relacionados ao aprimoramento da gestão de riscos foram tratados: identificação e avaliação de riscos, tratamento de riscos, monitoramento e controle de riscos, e documentação e comunicação de riscos. A partir dos resultados apresentados verificou-se a necessidade de aplicar a MGR-GRATIC em outros contextos reais, de forma contínua, a fim de registrar as lições aprendidas podendo agilizar o gerenciamento de riscos em aquisições de TIC nas instituições públicas brasileiras.

7.2 TRABALHOS RELACIONADOS

A primeira etapa deste estudo consistiu na realização de uma pesquisa bibliográfica com o objetivo de identificar na literatura científica as abordagens existentes para gerenciar riscos (capítulo 2). A partir da revisão bibliográfica foram encontrados inúmeros trabalhos relacionados com a metodologia de gestão de riscos proposta nesta dissertação. A tabela 23 apresenta os principais trabalhos relacionados.

Tabela 23 - Trabalhos Relacionados à Temática da Pesquisa

Item	Ano	Título	Descrição
T01	2014	Gestão de Riscos em Aquisições de TI: proposta de avaliação de maturidade do processo de aquisição de TI da IN04/SLTI no âmbito do INSS (SILVA, 2014).	Apresenta uma proposta de avaliação de maturidade para o Processo de Contratação de TI da Secretaria de Logística de Tecnologia da Informação (SLTI), tendo como estudo de caso o Instituto Nacional do Seguro Social (INSS). A avaliação da maturidade dos processos é realizada com foco na gestão de riscos e fornece informações que podem apoiar a organização a planejar, executar e monitorar suas atividades visando à obtenção dos seus objetivos e melhoria contínua.
T02	2015	Metodologia de auditoria com foco em processo e risco (OLIVEIRA JÚNIOR, 2015).	Metodologia orientada para a avaliação de riscos e controles com foco em processos de trabalho, finalísticos ou de apoio, que suportam o objeto de fiscalização, por meio da aplicação de procedimentos e técnicas para mapear os processos envolvidos, seus objetivos, riscos e controles associados.
T03	2016	Metodologia de Gestão de Riscos de Segurança da Informação e Comunicação do	Propõe a padronização e sistematização da gestão de riscos de segurança da informação e comunicação na Administração Pública Federal

		SISP (MPOG, 2016).	
T04	2017	Proposta de metodologia de gestão de riscos para as contratações de TI da Funasa. (NOBRE, 2017).	Propõe a elaboração de uma metodologia para a gestão de riscos dos processos de aquisições de TI da Fundação Nacional da Saúde (FUNASA).
T05	2017	Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão (MPOG, 2017).	Propõe orientar, sistematizar e padronizar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos das unidades do Ministério do Planejamento a partir do método de priorização de processos organizacionais, bem como instruir sobre o monitoramento e reporte.
T06	2017	Metodologia de Gestão de Riscos do Instituto Brasileiro de Gestão Corporativa (IBGC, 2017).	Estabelece o nível de maturidade das instituições a partir da definição dos objetivos estratégicos e também do mapa de riscos da organização. Identifica o grau de apetite a riscos da organização e as faixas de tolerância e desvios em relação aos níveis de riscos aceitáveis.
T07	2017	Perception of Enterprise Risk Management in Brazilian Higher Education Institutions (ALVES, 2017).	Pesquisa para captar a percepção de como os principais gestores das universidades federais do setor público percebem a gestão de riscos de forma a fornecer informações sobre as lacunas de desenvolvimento do gerenciamento de riscos empresariais e software relacionado.
T08	2018	Metodologia de Gestão de Riscos da Controladoria Geral da União (CGU, 2018).	Orienta as unidades a implementar a metodologia de gestão de riscos em conformidade com a sua política de gestão de riscos.
T09	2018	Metodologia de Gestão de Riscos do Tribunal de Contas da União (TCU, 2018).	Utiliza uma estratégia de gestão de riscos iterativa baseada em ciclos sucessivos com complexidade crescente. Os objetos de gestão de riscos pode ser qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos do TCU.
T10	2018	Gestão de Riscos nas instituições universitárias: uma análise comparativa da metodologia da controladoria geral da união e do ministério do planejamento, desenvolvimento e gestão (SOUSA, 2018).	Compara as metodologias apresentadas pela Controladoria-Geral da União e pelo Ministério do Planejamento, Desenvolvimento e Gestão e verifica a possibilidade de adaptação destas à gestão universitária.

T11	2019	ForRisco: gerenciamento de riscos em instituições públicas na prática (BERMEJO et al., 2019).	Guia prático para a gestão de riscos de forma abrangente podendo ser usado para a instituição como um todo ou somente para uma unidade organizacional específica. Propõe a adoção da gestão de riscos como método de gestão complementar para organizações públicas podendo contribuir para maior desempenho organizacional por permitir controles e acompanhamentos sistêmicos nestes riscos. É a metodologia de gestão de riscos adotada pela maioria dos institutos federais de educação. Aborda a gestão de riscos de forma ampla.
T12	2019	Metodologia de Gestão de Riscos do IBGE (IBGE, 2019).	Aborda os riscos associados à estratégia, bem como os planos e objetivos institucionais, identificados tanto em programas e projetos (riscos estratégicos), como em processos e atividades (riscos operacionais e riscos para a integridade).

Conforme pode ser observado na tabela 23 os trabalhos apresentados na literatura abordam a temática do estudo de forma estruturada e padronizada. Sobre as publicações apresentadas vale destacar três trabalhos correlatos a este estudo, o primeiro apresentado por Nobre (2017), o segundo por Sousa (2018) e o terceiro por Bermejo (2019).

Nobre (2017) propõe uma abordagem sistêmica, apresentando conceitos, processos, atividades, tarefas e artefatos para integrar a gestão de riscos das contratações de TI, contribuindo para a normatização de procedimentos e a melhoria nos resultados das contratações de TI dentro da realidade da FUNASA. Os resultados apresentados pelo autor demonstram que a metodologia proposta apresenta viabilidade para sua utilização nos órgãos públicos federais, como meio de auxiliar a internalização de procedimentos previstos na legislação e o aprofundamento sobre o tema gerenciamento de riscos nas contratações de TI na Administração Pública Federal (APF).

No entanto, Nobre (2017) utiliza a legislação que atualmente foi revogada e normas sobre gestão de riscos que foram atualizadas nos últimos anos. Tendo em vista que a gestão de riscos deve acompanhar o contexto interno e externo da instituição, a abordagem feita por este autor é diferente da proposta deste estudo, uma vez que não aborda o compartilhamento e aprendizado contínuo de forma transparente no decorrer o processo licitatório.

O estudo de Sousa (2018) por sua vez, compara as metodologias apresentadas pela Controladoria-Geral da União (CGU, 2018) e pelo Ministério do Planejamento, Desenvolvimento e Gestão (MPOG, 2017) e verifica a possibilidade de adaptação destas à gestão universitária. Este autor identifica as convergências e/ou as divergências na estrutura, processos e metodologias.

Sousa (2018) conclui que as metodologias elaboradas pela CGU e pelo MPOG apresentam semelhanças por possuírem embasamentos teóricos e legal similares. Este autor afirma que é possível a aplicação das metodologias na gestão de riscos das instituições universitárias, contudo, existe a necessidade de adaptação, respeitando as devidas particularidades da gestão universitária.

As metodologias comparadas por Sousa (2018) foram desenvolvidas de forma a abranger a gestão de riscos dentro da organização como um todo, não apresenta um inventário contendo diversos riscos já identificados por outras instituições e nem um repositório para compartilhamento de informações sobre contratações já realizadas o que difere deste estudo.

Bermejo et al. (2019) definiram um guia sobre gestão de riscos em organizações do setor público de forma a promover e motivar as melhores práticas de gerenciamento de riscos através de uma metodologia própria trazendo um conjunto de ferramentas para administrar e controlar os riscos. Com a solução ForRisco os autores afirmam que é possível organizar e planejar recursos de forma a reduzir os impactos dos riscos na instituição.

Porém Bermejo et al. (2019) destacam que o estabelecimento de uma metodologia-padrão para todas as instituições públicas somente seria efetivo se tivessem as mesmas características. Entretanto, observa-se que cada instituição, dentro da sua autonomia, desenvolve a sua administração em conformidade com as suas demandas locais e seguindo características próprias.

Estes autores afirmam que as metodologias de gestão de riscos possuem diversas similaridades entre si, especialmente por identificarem e tratarem as incertezas de forma sistemática para que haja uma comunicação precisa ao longo do processo de avaliação de riscos. Observa-se que a diferença entre as metodologias de gestão de riscos está relacionada à aplicação prática. Por ser algo

particular, a gestão de riscos deve ser elaborada sob medida para cada Instituição (BERMEJO et al., 2019).

Bermejo et al. (2019) consideram que analisar metodologias diferentes pode enriquecer e agregar valor na condução da gestão de riscos. O IBGC (2017) ressalta que é importante que as organizações, ao considerarem a adoção ou construção de um modelo ou metodologia de gestão de riscos, analisem o ambiente e o mercado em que atuam, assim como seu entendimento sobre gerenciamento de riscos e as variáveis influenciadoras.

A metodologia proposta por Bermejo et al. (2019) difere da solução apresentada neste estudo pois não possui um catálogo com riscos e controles já identificados por especialistas na área, como também não dispõe de um repositório digital de informações para o compartilhamento do aprendizado durante a execução do processo de aquisição de TIC

7.3 LIMITAÇÕES DA PESQUISA

A pesquisa foi realizada em conformidade com o método *Design Science Research*. O estudo apresenta limitações em relação ao público-alvo escolhido e escopo de atuação. O público-alvo para realização do estudo de caso foi a equipe de planejamento da contratação de TIC, formada por oito pessoas de apenas um Instituto Federal de Educação. Neste sentido, devem ser observadas e consideradas as seguintes limitações:

a) As informações obtidas através dos questionários e entrevistas estão limitadas a opiniões pessoais dos participantes desta pesquisa, restritas a experiências práticas obtidas por meio de participação em diversos processos de aquisição de TIC.

b) O estudo de caso foi realizado apenas em um Instituto Federal de Educação, é importante a realização de avaliações em outras instituições públicas brasileiras, pois cada equipe de planejamento da contratação tem suas características, habilidades e competências que influenciam o resultado final do processo.

c) O estudo de caso considerou apenas o ponto de vista dos especialistas que atuam diretamente com aquisições de TIC e que participam da equipe de planejamento da contratação, podendo não representar a opinião dos demais atores envolvidos no processo de aquisição.

d) O estudo de caso utilizou processos de aquisição relativamente simples e com pouca complexidade de serem conduzidos pela equipe de planejamento da contratação. A aplicação da MGR-GRATIC em outros processos de aquisição é necessária para a melhoria contínua da solução proposta neste estudo.

7.4 CONTRIBUIÇÕES

A pesquisa propôs uma abordagem prática e sistematizada para gestão de riscos apresentando fases, técnicas, ferramentas, artefatos e procedimentos aplicados ao processo de aquisição de TIC no contexto das instituições públicas brasileiras. Os especialistas na área de contratações de TIC participantes do estudo de caso concordaram com a viabilidade prática para sua implementação.

A metodologia proposta neste estudo é embasada no processo de aquisição de TIC adotado pelo governo federal e está em conformidade com as Instruções Normativas SGD/ME Nº 1/2019 (BRASIL, 2019b), MPOG Nº 5/2017 (BRASIL, 2017) e MP/CGU Nº 1/2016 (BRASIL, 2016). Neste sentido, pode ser adaptada para uso não somente o cenário educacional, mas também em outros contextos públicos, uma vez que as fases definidas foram propostas em conformidade com a legislação vigente e abordagens adotadas pelo setor público.

Outra contribuição importante do trabalho é a reunião de riscos e controles já estabelecidos pelos órgãos públicos através do inventário de riscos disponibilizado na planilha documentadora (mapa de gerenciamento de riscos) que compõem a metodologia de gestão de riscos GRATIC. Este catálogo de riscos e controles a serem aplicados possibilita a realização da gestão de riscos sem depender de um especialista na área, uma vez que já foram registrados vários riscos como também diversas possibilidades de controle e tratamento. O link de acesso a planilha está disponibilizado no apêndice H.

A MGR-GRATIC, apresentada no estudo de caso aumenta a transparência dos atos administrativos referente ao gerenciamento de riscos, uma vez que define fases padronizadas que são documentadas e informadas em todas as fases do processo de aquisição de TIC. Observa-se ainda que a solução proposta por este estudo possibilita de forma efetiva acompanhar e controlar os riscos de maneira estruturada por meio do painel evolutivo de riscos e indicadores de desempenho da gestão de riscos no processo de aquisição de TIC.

Além disso, a metodologia desenvolvida disponibiliza um repositório digital de informações para registro de lições aprendidas ao longo da realização da gestão de riscos em aquisições de TIC. Este artefato contém diversas publicações realizadas no âmbito acadêmico e governamental, como também disponibiliza os documentos utilizados pela MGR-GRATIC.

7.5 PERSPECTIVAS FUTURAS

Os resultados deste estudo poderão contribuir para trabalhos futuros que abordem temas relacionados à gestão de riscos em aquisições de TIC, como por exemplo:

a) Disponibilização de uma base de conhecimento em um repositório digital de informações (base de conhecimento corporativo) sobre gestão de riscos acessível a todas as instituições públicas brasileiras, sobre riscos, ameaças, vulnerabilidades, controles e ações de mitigação realizadas em processos de aquisição de TIC, de forma que lições aprendidas possam ser aproveitadas para outros processos podendo agilizar o gerenciamento de riscos em aquisições de TIC.

b) Desenvolvimento de um software específico para apoiar a gestão de riscos em aquisições de TIC envolvendo as instituições públicas no cenário público brasileiro.

c) Disponibilização de um observatório central para monitoramento e controle de riscos em todos os processos licitatórios realizados por todas as organizacionais públicas brasileiras.

d) Realização de estudos de caso em outras instituições públicas brasileiras visando o aprimoramento do inventário de riscos e controles adotados pela MGR-GRATIC.

REFERÊNCIAS

ALVES, Gustavo de Freitas; Neto, Waldemar Lima; COLI JUNIOR, Marçal Chagas; BERMEJO, Paulo Henrique de Souza; SANTA' ANA, Tomás Dias; SALGADO, Eduardo Gomes. **Perception of Enterprise Risk Management in Brazilian Higher Education Institutions**. 14th European, Mediterranean, and Middle Eastern Conference on Information Systems –EMCIS 2017, Coimbra, 2017. LNBIP, v.299, p 506-512. 2017. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-65930-5_40 Acesso em: 1 set. 2019.

BARROS, Aidil J. da S.; LEHFELD, Neide Aparecida de S. **Fundamentos de Metodologia Científica.** 3ª ed. São Paulo: Pearson Prentice Hall, 2007.

BERMEJO, Paulo Henrique de Souza et al. **ForRisco: Gerenciamento de Riscos em Instituições Públicas.** 2ª ed. Brasília-DF: Ed. Evobiz, 2019. Disponível em: http://www.forpdi.org/forrisco/livrov2.pdf Acesso em: 2 ago. 2019.

BRASIL. **Portal de Compras**. Brasília, DF: Governo Federal, 2019. Disponível em: https://www.comprasgovernamentais.gov.br Acesso em: Nov. 2019d.

BRASIL. **Decreto Nº 9.203/2017, de 22 de novembro de 2017.** Brasília, DF, 2017.

BRASIL. **Decreto Nº 10.024, de 20 de setembro de 2019**. Brasília, DF, 2019.

BRASIL. **Guia de orientação para gestão de riscos. v. 1.0.** Brasília, DF, 2013. Disponível em: http://www.gespublica.gov.br/sites/default/files/documentos/p_vii_risco_oportunidade.pdf Acesso em: 3 out. 2019.

BRASIL. **Instrução Normativa Conjunta MP/CGU Nº 1/2016 de 10 de maio de 2016**. Brasília, DF, 2016.

BRASIL. **Instrução Normativa ME/SG Nº 1/2019 de 10 de janeiro de 2019**. Brasília, DF, 2019.

BRASIL. **Instrução Normativa ME/SGD Nº 1/2019 de 4 de abril de 2019.** Brasília, DF, 2019b.

BRASIL. **Instrução Normativa ME/SGD Nº 2/2019 de 20 de setembro de 2019.** Brasília, DF, 2019c.

BRASIL. **Instrução Normativa MPOG Nº 5/2017 de 25 de maio de 2017.** Brasília, DF, 2017.

BRASIL. **Lei Nº 8.666**, de 21 de junho de 1993. Brasília, DF, 1993.

BRASIL. **Lei Nº 10.520**, de 17 de julho de 2002. Brasília, DF, 2002.

BRASILIANO, Antônio Celso Ribeiro. **Inteligência em Riscos: Gestão Integrada em Riscos Corporativos.** 2ª ed. rev. e ampl. São Paulo: Sicurezza, 2018.

CONTROLADORIA GERAL DA UNIÃO. **Metodologia de Gestão de Riscos**. Brasília, DF, 2018. Disponível em:

https://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf Acesso em: 7 jul. 2019.

_____. **Guia Prático de Gestão de Riscos para Integridade: Orientações para a Administração Pública Federal, Direta, Autárquica e Fundacional.** Brasília, DF, 2018b. Disponível em: http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual-gestao-de-riscos.pdf Acesso em: 13 set. 2019.

_____. **Gestão de Riscos da CGU**. Brasília, DF, 2018c. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/29486/4/Apresentacao_Formacao_de_Multiplicadores.pdf Acesso em: 14 set. 2019.

COSO. **Enterprise Risk Management: Integrated Framework. Executive Summary**. PricewaterhouseCoopers, 2004. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf Acesso em: 20 jun. 2019.

COSO. **Gerenciamento de Riscos Corporativos: Estrutura Integrada.** 2007. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf Acesso em: 5 jun.2019.

COSO. **Enterprise Risk Management, Integrating with Strategy and Performance Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission.** 2017. Disponível em: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Acesso em: 7 jul. 2019.

CRUZ, Cláudio Silva da, Rejane Maria da Costa Figueiredo e Edméia Leonor Pereira de Andrade. **Processo de Contratação de Serviços de Tecnologia da Informação para Organizações Públicas.** MCT/SPI, Brasília, DF, 2011.

CRUZ, Cláudio Silva da. **Governança de TI e Conformidade Legal no Setor Público: um quadro referencial normativo para a contratação de serviços de TI.** Dissertação de Mestrado, Universidade Católica de Brasília, Brasília, DF, 2008.

CRUZES, Daniela S.; DYBA, Tore. **Recommended Steps for Thematic Synthesis in Software Engineering.** In: Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on. IEEE, 2011.

DALLAS, Michael. **Management of Risk: Guidance for Practitioners and the International Standard on Risk Management, ISO 31000: 2009.** The Stationary Office, 2013.

DRESCH, Aline. **Design Science e Design Science Research como Artefatos Metodológicos para Engenharia de Produção**. Dissertação de mestrado. Unisinos, 2013. Disponível em: http://biblioteca.asav.org.br/vinculos/000003/0000030A.pdf Acesso em: 9 out. 2019.

DRESCH, Aline; LACERDA, Daniel Pacheco; ANTUNES, José Antônio Valle Júnior. **Design Science Research: Método de Pesquisa para Avanço da Ciência e Tecnologia.** Porto Alegre, RS: Editora Bookman, 2015.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). **Gestão de Riscos no Setor Público.** Brasília, DF, 2019. Disponível em: https://www.escolavirtual.gov.br Acesso em: 9 jul. 2019.

FERMA. **Norma de Gestão de Riscos.** FERMA, 2003. Disponível em: https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-portuguese-version.pdf Acesso em: 10 out. 2019.

FRANCO, Fernando. **Governança e Gestão de Riscos em Organizações Públicas.** Brasília, DF, 2017. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwj75-DeofPiAhWyxVkKHWrSApQQFjAAegQIBRAC&url=http%3A%2F%2Fbrasilia.mackenzie.br%2Fapps%2Ffiles%2Ffpmb_governanca_e_gestao_de_riscos_em_organizacoes_publicas_apostila.pdf&usg=AOvVaw1TnGu048CEPZRgbS8CkNAF Acesso em: 6 jun. 2019.

GUARDA, Graziela Ferreira. **Análise de Contratos de Terceirização de TI na Administração Pública Federal sob a Ótica da Instrução Normativa Nº 04.** Dissertação de Mestrado. UNB, Brasília, 2011.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social.** 7ª ed. São Paulo, SP: Atlas, 2019.

HM GOVERNMENT (HMG) **The Orange Book: Management of Risk (Principles e Concepts).** 2019. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/815635/Orange_Book_Management_of_Risk.pdf Acesso em: 15 jul. 2019.

HM TREASURY (HMT). **The Orange Book: Management of Risk Principles and Concepts.** London: HM Treasury, 2004.

HOPKIN, Paul. **Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management**. 5ª ed. IRM. KoganPage, 2018.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Metodologia de Gestão de Riscos do IBGE. Brasília, DF: IBGE, 2019. Disponível em: https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/MetodologiaRiscos.pdf Acesso em: 20 nov. 2019.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia**. São Paulo, SP: IBGC, 2017. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21794/Riscos%20cad19.pdf Acesso em: 11 ago. 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Guide 73. Gestão de riscos: Vocabulário, Recomendações para uso em Normas**. 2005.

_____. **Risk Management: Principles and Guidelines**. 2009.

_____. **31000:2018: Risk Management (Guidelines, Provides Principles, Framework and a Process for Managing Risk).** 2018.

_____. **31010:2019: Risk Management (Risk Assessment Techniques).** 2019.

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Subcomitê de Normas de Controle Interno. **Diretrizes para Normas de**

Controle Interno do Setor Público: Informações Adicionais sobre Gestão de Risco nas Entidades. INTOSAI GOV 9130. Áustria, 2007. Tradução: Antônio Alves de Carvalho Neto. Brasília, 2013.

INSTITUTE OF RISK MANAGEMENT (IRM). **A Risk Management Standard**. 2002. Disponível em: https://www.theirm.org/media/6827/arms_2002_irm.pdf Acesso em: nov. 2019.

ISACA. **COBIT 5: For Risk.** USA, 2013. Disponível em: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf Acesso em: 3 jul. 2019.

LACERDA, D. P.; DRESCH, A.; PROENÇA, A; JÚNIOR, J. A. V. A. **Design Science Research: Método de Pesquisa para a Engenharia de Produção.** Gest. Prod., São Carlos, v. 20, n. 4, p. 741-761, 2013. Disponível em: http://www.scielo.br/pdf/gp/v20n4/aop_gp031412.pdf Acesso em: 13 ago. 2019.

KAUARK, Fabiana da Silva; MANHÃES, Fernanda Castro; MEDEIROS, Carlos Henrique. **Metodologia da Pesquisa: Um Guia Prático.** Itabuna: Via Litterarum, 2010.

LIKERT, R. **A Technique for the Measurement of Attitudes.** Archives of Psychology. v. 22, n. 140, p. 44-53, 1932.

MANSON, N. J. **Is Operations Research Really Research?.** Operations Research Society of South Africa. v. 22, n.2, p. 155-180, 2006.

MARCH, S. T.; SMITH, G. F. **Design and Natural Science Research in Information Technology.** Decision Support Systems, v. 15, p. 251-266, 1995. Disponível em: http://dx.doi.org/10.1016/0167-9236(94)00041-2 Acesso em: 5 out. 2019.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia de Trabalho Científico**. 8ª ed. Editora: Atlas, 2017.

MARCH, S. T.; STOREY, V. C. **Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research.** MIS Quarterly, v. 32, n. 4, p. 725-730, 2008.

MYERS, M. and Venable, J. 2014. **A Set of Ethical Principles for Design Science Research in Information Systems. Information & Management.** 51 (6): pp. 801-809.

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO e GESTÃO (MPOG). **Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação.** v 3.0. Brasília, DF: MPOG, 2017. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjXmrmH_-niAhVICrkGHQTKCpUQFjAAegQIAhAC&url=https%3A%2F%2Fwww.governodigital.gov.br%2Fdocumentos-e-arquivos%2FGuia_de_Boas_Praticas_v3.pdf&usg=AOvVaw2822VEUP_TEqqYK0qShBJm Acesso em: 16 jun. 2019.

_____. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília, DF: MPOG, 2017b. Disponível em:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwith4ywy7fjAhWUILkGHW1MAGoQFjAAegQIBRAC&url=http%3A%2F%2Fwww.planejamento.gov.br%2Fassuntos%2Fgestao%2Fcontrole-interno%2Fmanual-de-girc&usg=AOvVaw15Ux85j0KP0dDvDxup1TBN Acesso em: 7 jul. 2019.

_____. **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal.** Brasília, DF: MPOG, 2016. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/MGR-SISP-V260816.pdf/at_download/file Acesso em: 13 ago. 2019.

NOBRE, Leonardo Santana. **Proposta de Metodologia de Gestão de Riscos para as Contratações de TI da Funasa.** Dissertação de Mestrado Profissional em Computação Aplicada. UNB, Brasília, DF, 2017. Disponível em: http://www.repositorio.unb.br/bitstream/10482/25305/1/2017_LeonardoSantanaNobre.pdf Acesso em: 21 jun. 2019.

OFFICE OF GOVERNMENT COMMERCE (OGC). **Management of Risk: Guidance for Practitioners.** Office of Government Commerce - Axelos, London 2010.

PARDINI, Eduardo Person. **E-book Gestão de Riscos.** Disponível em: https://www.legiscompliance.com.br/images/pdf/ebook_pardini.pdf Acesso em: 11 nov. 2019.

PARREIRA, Glauco Cintra. **Modelo de Decisão para Gestão de Riscos de Contratos de Serviços de TI no Poder Judiciário Brasileiro.** Dissertação de Mestrado, UNB, Brasília, DF, 2018. Disponível em: https://repositorio.unb.br/handle/10482/33993 Acesso em: 22 out. 2019.

PEFFERS, Ken et al. **A Design Science Research Methodology for Information Systems Research.** Journal of Management Information Systems, v. 24, n. 3, p.45-77, 2007. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.535.7773&rep=rep1&type=pdf Acesso em: 9 jul. 2019.

PIMENTEL, Mariano; FILIPPO, Denise; SANTORO, Flávia Maria. (2019). **Design Science Research: fazendo pesquisas científicas rigorosas atreladas ao desenvolvimento de artefatos computacionais projetados para a educação.** In Metodologia de Pesquisa Científica em Informática na Educação: Concepção de Pesquisa. 1. ed. Porto Alegre: SBC, 2019. Disponível em: https://metodologia.ceie-br.org/wp-content/uploads/2018/10/cap1_5.pdf. Acesso em: 26 jul. 2019.

PIRES, Tatieures G.; CAVALCANTE, Sueli M. de; CORRÊA, Denise M. M. C.; NETO, Denise M. M. C. **Gestão de Riscos nas Aquisições de Soluções de TI: Uma Análise Crítica dos Modelos de Boas Práticas.** Anais do EATI - Encontro Anual de Tecnologia da Informação e STIN – Simpósio de Tecnologia da Informação da Região Noroeste do RS, 2016. Disponível em: http://eati.info/eati/2016/assets/anais/Longos/93.pdf Acesso em: 9 mai. 2019.

PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge.** Project Management Institute. Fifth Edition Pennsylvania USA, 2013.

_____. **A Guide to the Project Management Body of Knowledge.** Project Management Institute. Sixth Edition, Pennsylvania USA, 2017.

SIAU, Keng; ROSSI, Matti. **Evaluation Techniques for Systems Analysis and Design Modelling Methods – A review and Comparative Analysis**. Information Systems Journal, 1-20. USA, 2007. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1365-2575.2007.00255.x Acesso em: 17 nov. 2019.

SILVA, Dyego Alves da; OLIVEIRA, Edgard Costa de; CANEDO, Edna Dias. **Avaliação de Riscos do Processo de Planejamento da Contratação de TI: Uma Proposta para Órgãos Governamentais Brasileiros.** Revista Brasileira de Sistemas de Informação. Rio de Janeiro, vol. 9 Nº 1, pp. 168-186. 2016. Disponível em: http://www.seer.unirio.br/index.php/isys/article/download/5322/5043 Acesso em: 26 jun. 2019.

SILVA, Hildiene Castro. **Gestão de Riscos em aquisições de TI: proposta de avaliação de maturidade do processo de contratação de TI da IN04/SLTI no âmbito do INSS**. Dissertação de Mestrado, UNB, Brasília, DF, 2014.

SOARES NETTO, Antônio Fernandes. **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, UNB, Brasília, DF, 2013.

SOUSA, Monique Regina Bayestorff Duarte de; FINATI, Caroline Renata Delle; PEREZ, Manuela; DUARTE, Karen Sabrina Bayestorff. **Gestão de Risco nas Instituições Universitárias: Uma Análise Comparativa da Metodologia da Controladoria Geral da União e do Ministério do Planejamento, Desenvolvimento e Gestão.** XVIII Colóquio Internacional de Gestión Universitaria. Campus UTPL, 2018. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/190666/102_00046.pdf?sequence=1 Acesso em: 11 jul. 2019.

SOUZA, Kleberson; BRASIL, Franklin. **Como Gerenciar Riscos na Administração Pública: Estudo Prático em Licitações.** Curitiba, PR: Editora Negócios Públicos do Brasil, 2017.

TRIBUNAL DE CONTAS DA UNIÃO. **Gestão de Riscos: Roteiro de Avaliação de Maturidade da Gestão de Riscos.** Brasília-DF: TCU, 2018. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=2ahUKEwj9lePgoPHiAhVbIbkGHQ2gCp0QFjAGegQIBBAC&url=https%3A%2F%2Fportal.tcu.gov.br%2Flumis%2Fportal%2Ffile%2FfileDownload.jsp%3FfileId%3D8A81881E61E3109601620CBEC2333A04&usg=AOvVaw1W2LwFjY-auqJ-ggN8WwwK Acesso em: 9 jun. 2019.

_____. **Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação: Riscos e Controles para o Planejamento da Contratação. Versão 1.0.** Brasília, DF: TCU, 2012. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC82195464&inline=1 Acesso em: 26 jun. 2019.

_____. **Manual de Gestão de Riscos do TCU.** Brasília, DF: TCU, 2018b. Disponível em: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/ Acesso em: 8 jul. 2019.

_____. **Referencial Básico de Gestão de Riscos.** SEGECEX/COGER. Brasília-DF: TCU, 2018c. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm Acesso em: 30 jun. 2019.

_____. **Relatório Individual dos Respondentes do Levantamento Integrado de Governança Organizacional Pública: Arquivos Individuais.** Brasília, DF: TCU, 2018g. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E67991D32016799A2A9634CB7 Acesso em: 7 out. 2019.

_____. **Relatório Técnico Completo de Acompanhamento IGG 2018.** Brasília, DF: TCU, 2018f. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F6B4849B5016B9505FC5A254F Acesso em: 28 nov. 2019.

_____. **Relatório Técnico Detalhado (ciclo 2017).** Brasília, DF: TCU, 2017. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F62B15ED20162E39DB9C50879 Acesso em: 26 out. 2019.

_____. **Resultados do Levantamento Integrado de Governança Organizacional Pública - ciclo 2017.** Brasília, DF: TCU, 2017. Disponível em:https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-2017/ Acesso em: 1 jul. 2019.

_____. **Resultados do Levantamento Integrado de Governança Organizacional Pública - ciclo 2018.** Brasília, DF: TCU, 2018d. Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-2018/resultados.htm Acesso em: 9 jul. 2019.

_____. **Riscos e Controles nas Aquisições.** Disponível em: https://portal.tcu.gov.br/comunidades/controle-externo-das-aquisicoes-logisticas/atuacao/riscos-e-controles-nas-aquisicoes/ Brasília, DF: TCU, 2013. Acesso em: 6 set. 2019.

_____. **Sumários Executivos: Acompanhamento de Governança Pública Organizacional 2018**. Brasília, DF: TCU, 2018e Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F6B4849B5016B949ED3694B30 Acesso em: 20 jun. 2019.

TRIBUNAL ELEITORAL DO PARÁ. **Plano de Tratamento de Riscos para as Aquisições.** Belém, PA: TRE-PA, 2018. Disponível em: http://www.justicaeleitoral.jus.br/arquivos/tre-pa-plano-de-tratamento-de-riscos-completo-versao-ii Acesso em: 20 nov. 2019.

TRIBUNAL REGIONAL DO TRABALHO 8ª Região. **Plano de Tratamento de Riscos nas Aquisições e Contratações. 2017.** Belém, PA: TRT-PA, 2017. Disponível em: https://www.trt8.jus.br/sites/portal/files/roles/governanca/plano_de_tratamento_de_riscos_nas_aquisicoes_e_contratacoes.pdf Acesso em: 15 abr. 2019.

_____. 13ª Região. **Guia de Boas Práticas de Contratação de Soluções de TIC.** João Pessoa, PB: TRT-PB, 2017. Disponível em: https://www.trt13.jus.br/institucional/governanca/publicacoes/trt-13/setic/escritorio-de-processos/processo-de-contratacao-de-tic/guia-de-boas-praticas-de-contratacoes-de-tic.pdf Acesso em: 2 nov. 2019.

VAISHNAVI, V.; KUECHLER, W. **Design Research in Information Systems.** 2005. Disponível em: http://desrist.org/design-research-in-information-systems. Acesso em: 3 jul. 2019.

WESTERMAN, G., HUNTER, R. **O Risco de TI.** São Paulo. Editora Master Books, 2008.

WHOLIN, C. RUNESON, P. HOST, M. OHLSSON, M.C. REGNELL, B., WESSLEN, A. **Experimentation in Software Engineering**. Springer, 2012.

WIERINGA, R. J. **What is Design Science?** In: WIERINGA, R. J. Design Science Methodology for Information Systems and Software Engineering. [S.l.]: Springer Berlin Heidelberg, 2014.

VIEIRA, James Batista; BARRETO, Rodrigo Tavares de Souza. **Governança, Gestão de Riscos e Integridade.** Brasília, DF: ENAP, 2019. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4281/1/5_Livro_Governan%C3%A7a%20Gest%C3%A3o%20de%20Riscos%20e%20Integridade.pdf Acesso em: 5 out. 2019.

YIN, Robert K. **Estudo de Caso: Planejamento e Métodos.** 5ª ed. Porto Alegre, RS: Bookman, 2015.

APÊNDICE A – PARTICIPANTES DA PESQUISA

INSTITUIÇÕES FEDERAIS DE EDUCAÇÃO - PARTICIPANTES DA PESQUISA

Fonte: Plataforma Nilo Peçanha – ano 2019 (ano base 2018)

Relatório Individual da auto avaliação apresentado através do acórdão 2699/2018)

4331 - Riscos da área de gestão de contratações são geridos

Instituição	Perfil	IGOV-TCU/2018 RiscoContr
IF01	Instituição situada na região norte do Brasil, com 5.832 alunos matriculados, 79 cursos e 6 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 373 professores, 381 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 112.069.434,00.	Inexpressivo (0 a 14,9%)
IF02	Instituição situada na região norte do Brasil, com 19.086 alunos matriculados, 258 cursos e 15 unidades. Oferta cursos de técnico, graduação e pós-graduação. Possui 1006 professores, 894 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 378.736.833,00.	Inicial (15 a 39,9%)
IF03	Instituição situada na região nordeste do Brasil, com 16.428 alunos matriculados, 220 cursos e 15 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 849 professores, 864 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 321.443.024,00.	Inexpressivo (0 a 14,9%)
IF04	Instituição situada na região nordeste do Brasil, com 33.125 alunos matriculados, 251 cursos e 21 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1715 professores, 1101 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 571.248.890,00.	Inexpressivo (0 a 14,9%)
IF05	Instituição situada na região centro-oeste do Brasil, com 18.870 alunos matriculados, 216 cursos e 10 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 712 professores, 563 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 219.785.759,00.	Aprimorado (70 a 100%)
IF06	Instituição situada na região sul do Brasil, com 17.528 alunos matriculados, 214 cursos e 15 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1038 professores, 864 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 368.814.582,00.	Intermediário (40 a 69.9%)
IF07	Instituição situada na região nordeste do Brasil, com 51.413 alunos matriculados, 686 cursos e 32 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1846 professores, 1595 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 696.349.669,00.	Inexpressivo (0 a 14,9%)
IF08	Instituição situada na região sudeste do Brasil, com 35.664 alunos matriculados, 330 cursos e 22 unidades. Oferta cursos de básico propedêutico, qualificação profissional, técnico, graduação e pós-graduação. Possui 1637 professores, 1358 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 662.212.441,00.	Inicial (15 a 39,9%)

IF09	Instituição situada na região centro-oeste do Brasil, com 17.655 alunos matriculados, 242 cursos e 14 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1302 professores, 893 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 451.951.673,00.	Inexpressivo (0 a 14,9%)
IF10	Instituição situada na região centro-oeste do Brasil, com 28887 alunos matriculados, 301 cursos e 19 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1232 professores, 845 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 444.373.803,00.	Inexpressivo (0 a 14,9%)
IF11	Instituição situada na região nordeste do Brasil, com 27831 alunos matriculados, 242 cursos e 21 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1324 professores, 1031 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 539.504.649,00.	Inexpressivo (0 a 14,9%)
IF12	Instituição situada na região nordeste do Brasil, com 27.086 alunos matriculados, 283 cursos e 16 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1324 professores, 1014 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 572.843.951,00.	Inexpressivo (0 a 14,9%)
IF13	Instituição situada na região nordeste do Brasil, com 25.018 alunos matriculados, 353 cursos e 20 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1349 professores, 947 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 424.630.401,00.	Inexpressivo (0 a 14,9%)
IF14	Instituição situada na região norte do Brasil, com 17.626 alunos matriculados, 175 cursos e 9 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 700 professores, 651 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 222.829.648,00.	Inexpressivo (0 a 14,9%)
IF15	Instituição situada na região nordeste do Brasil, com 44.102 alunos matriculados, 533 cursos e 20 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 1.628 professores, 1.159 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 608.567.739,00.	Inexpressivo (0 a 14,9%)
IF16	Instituição situada na região nordeste do Brasil, com 50.335 alunos matriculados, 721 cursos e 23 unidades. Oferta cursos de básico propedêutico, qualificação profissional, técnico, graduação e pós-graduação. Possui 1.605 professores, 1.144 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 587.247.076,00.	Aprimorado (70 a 100%)
IF17	Instituição situada na região sudeste do Brasil, com 12.903 alunos matriculados, 183 cursos e 9 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 620 professores, 570 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 239.571.299,00.	Inicial (15 a 39,9%)
IF18	Instituição situada na região norte do Brasil, com 14.308 alunos matriculados, 147 cursos e 11 unidades. Oferta cursos de qualificação profissional, técnico, graduação e pós-graduação. Possui 721 professores, 584 técnicos-administrativos. O gasto total informado (pessoal, investimentos e outros custeios) é de R$ 244.417.798,00.	Inexpressivo (0 a 14,9%)

APÊNDICE B – PERFIL DOS PARTICIPANTES

PARTICIPANTES DOS QUESTIONÁRIOS 1 e 2

(Adaptado da Instrução Normativa Nº 1/2019 de 4 de abril de 2019)

Área	Papel	Responsabilidade
Área Requisitante (unidade do órgão ou entidade que demande a contratação de uma solução de TIC).	Integrante Requisitante	- Demandar a aquisição de TIC.
	Gestor do Contrato	- Coordenar e comandar o processo de gestão e fiscalização da execução contratual.
	Fiscal Requisitante do Contrato	- Fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC.
Área de Tecnologia da Informação (unidade setorial, seccional ou correlata do SISP, responsável por gerir a Tecnologia da Informação e Comunicação e pelo planejamento, coordenação e acompanhamento das ações relacionadas às soluções de TIC do órgão ou entidade).	Integrante Técnico	- Gerenciar a TI - Planejar, coordenar e acompanhar ações relacionadas a ti da instituição.
	Fiscal Técnico do Contrato	- Fiscalizar tecnicamente o contrato.
Área Administrativa (unidades setoriais e seccionais do Sistema de Serviços Gerais – SISG com competência para planejar, coordenar, supervisionar e executar as atividades relacionadas aos processos de contratação).	Integrante Administrativo	- Executar atividades para aquisição de TIC.
	Fiscal Administrativo do Contrato	- Fiscalizar o contrato quanto os aspectos administrativos.
Equipe de Planejamento da Contratação	Planejamento da Contratação	Planejar a contratação.

APÊNDICE C – DIAGNÓSTICO SITUACIONAL

QUESTIONÁRIO 1 – DIAGNÓSTICO SITUACIONAL SOBRE AQUISIÇÕES DE TIC

Segundo o relatório sobre governança pública divulgado pelo TCU em 2018 a maioria das instituições públicas brasileiras possui baixa capacidade de gerir contratações relacionadas à área de Tecnologia da Informação. Visando propor melhorias para o processo de aquisições de TIC, essa pesquisa visa compreender como sua instituição executa este processo na prática. Contamos com sua colaboração e desde já agradecemos sua participação.

Caso tenha dúvidas, por gentileza entre em contato: Fabiana -> telefone 063 98485-0805 (WhatsApp) ou ffc2@cin.ufpe.br

---

A. Identificação da Instituição

1. Qual instituição você trabalha? _____

2. Qual setor você trabalha?

( ) Tecnologia de Informática ( ) Governança ( ) Licitações ( ) Administração

3. Qual papel já exerceu no processo de aquisição de TIC?

( ) Integrante requisitante ( ) Integrante Técnico ( ) Fiscal Administrativo do Contrato ( ) Fiscal Técnico do Contato ( ) Nenhum ( ) Outro:_____

B. Jurisprudência

4. Nas aquisições de TIC de sua instituição é obrigatório o uso da Instrução Normativa SLTI/MP Nº 4, de 11 de setembro de 2014, você adota todas as práticas recomendadas?

( ) Sim ( ) Não ( ) Não sabe informar

5. Sua instituição já adota as recomendações da nova Instrução Normativa SGD/ME Nº 1, de 4 de abril de 2019?

( ) Sim ( ) Não ( ) Não sabe informar

C. Modelo de Aquisições de TIC

6. As aquisições de TIC de sua instituição são precedidas de planejamento, elaborada em harmonia com o Plano Diretor de Tecnologia da Informação (PDTI)?

( ) Sim ( ) Não ( ) Não sabe informar

7. Sua instituição possui Plano Anual de Contratações (PAC) conforme recomenda a Instrução Normativa SEGES/ME Nº 1, de 10 de janeiro de 2019?

( ) Sim ( ) Não ( ) Não sabe informar

8. Sua instituição adota as boas práticas recomendadas pelo guia de boas práticas em Contratação de TIC do Ministério do Planejamento, Desenvolvimento e Gestão?

( ) Sim ( ) Não ( ) Não sabe informar

9. Sua organização institui a equipe de planejamento da contratação de TIC?

( ) Sim ( ) Não ( ) Não sabe informar

10. Sua instituição cria todos os artefatos recomendados pelo guia de boas práticas do TCU?

( ) Sim ( ) Não ( ) Em parte ( ) Não sabe informar

11. Sua instituição divulga no site todos os artefatos gerados para cada processo de aquisição de TIC conforme recomenda a IN SGD/ME Nº 1, de 4 de abril de 2019?

( ) Sim ( ) Não ( ) Alguns ( ) Não sabe informar

12. Descreva em linhas gerais como é o processo de aquisição de TIC em sua instituição?

_____

D. Avaliação

13. Como você avalia o processo de aquisição de TIC de sua instituição?

( ) Péssimo ( ) Ruim ( ) Regular ( ) Bom ( ) Ótimo

14. Você considera necessário alguma melhoria para o processo de aquisição de TIC?

( ) Sim ( ) Não ( ) Talvez ( ) Não sabe informar

15. Quais são os problemas enfrentados em sua instituição para realizar aquisições de TIC?

_____

16. Na sua opinião, quais são as causas para a dificuldade em gerir riscos aquisições de TIC?

_____

17. O que você indicaria para melhoria do processo de aquisição de TIC?

_____

D. Monitoramento

18. O que você indicaria para melhorar o controle de qualidade do processo de aquisição de TIC?

_____

APÊNDICE D - DIAGNÓSTICO GESTÃO DE RISCOS

INSTITUTOS FEDERAIS DE EDUCAÇÃO

QUESTIONÁRIO 2 - DIAGNÓSTICO SOBRE GESTÃO DE RISCOS EM AQUISIÇÕES DE TIC

O levantamento sobre Governança Pública divulgado pelo Tribunal de Contas da União em 2018 aponta dados preocupantes sobre o processo de contratação de soluções de TIC e revela baixa maturidade em gestão de riscos em contratações públicas. Dentro deste cenário, este questionário pretende realizar um diagnóstico situacional que fará parte de uma pesquisa no Mestrado Profissional da Universidade Federal de Pernambuco visando propor melhorias para o processo de contratação de TIC no âmbito dos Institutos Federais de Educação. Este diagnóstico inicia com a visão de gestão de riscos dentro da organização, em seguida avalia como são realizadas as etapas deste processo: escopo, contexto e critério, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, comunicação e consulta e monitoramento e análise crítica. Com estas informações será proposta uma solução para a gestão de riscos no processo de aquisições de TIC.

Contamos com sua colaboração e desde já agradeço sua atenção.

Caso tenha dúvidas, por gentileza entre em contato: Fabiana -> telefone 063 98485-0805 (WhatsApp) ou ffc2@cin.ufpe.br

DADOS GERAIS

1. Nome da Instituição de Ensino? _____

2. Qual é a sua área de atuação?

( ) Tecnologia da Informação ( ) Governança ( ) Licitações ( ) Administrativa

3. Qual papel já exerceu no processo de aquisição de TIC?

( ) Integrante requisitante ( ) Integrante Técnico ( ) Fiscal Administrativo do Contrato ( ) Fiscal Técnico do Contato ( ) Nenhum ( ) Outro:_____

PROCESSO DE GESTÃO DE RISCOS

Segundo a norma ISO/IEC/ABNT 31000:2018 convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processo da organização.

4. Como sua instituição realiza a gestão de riscos no processo de aquisição de TIC?

( ) Usa uma metodologia própria de gestão de Riscos.

( ) Usa o plano de gestão de riscos definido pela instituição.

( ) Usa a política de gestão de riscos própria da Instituição.

( ) Usa as recomendações da IN 01/2019

( ) Outra opção:_____

5. Na sua opinião, quais são as etapas/fases de um processo de gerenciamento de riscos eficiente para aquisição de TIC?

_____

6. Sua instituição realiza a gestão de riscos em todas as fases do processo de aquisição de TIC?

( ) Sim ( ) Não ( ) Não sabe informar

7. Como você avalia a gestão de riscos em aquisições de TIC de sua instituição?

( ) Péssimo ( ) Ruim ( ) Regular ( ) Bom ( ) Ótimo

ESCOPO, CONTEXTO E CRITÉRIO

Consiste em compreender o ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

8. Na sua opinião quais são os problemas ocasionados pela falta de gestão de riscos dentro do processo de aquisição de TIC (TCU, 2012; 2017; 2018)? Você pode indicar mais de uma alternativa.

( ) Atraso na entrega da solução de TI em razão de excesso de questionamentos e impugnações.

( ) Aquisição de bens e serviços com preços praticados acima do mercado.

( ) Licitações fracassadas em razão requisitos técnicos não exequíveis.

( ) Licitações desertas em razão de falta de fornecedores interessados a participar do processo licitatório.

( ) Aquisição de solução de TI que não atende às necessidades que originou a contratação.

( ) Não sabe informar.

( ) Outro problema: _____

9. Em sua opinião qual variável tem maior influência sobre a gestão de riscos no processo de aquisições de TIC?

( ) Monitoramento e Controle ( ) Sistematização ( ) Avaliação ( ) Padronização ( ) Planejamento

( )Capacitação ( ) Documentação ( ) Transparência ( ) Outra: _____

IDENTIFICAÇÃO DE RISCOS

O propósito desta etapa é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes nesta etapa.

10. Quais técnicas sua instituição utiliza para identificar riscos relacionados à aquisição de TIC?

( ) Brainstorming.

( ) Entrevistas Estruturadas ou semiestruturadas.

( ) Checklist.

( ) Técnica Estruturada de What If? (SWIFT).

( ) Análise Preliminar de Perigos (APP).

( ) Não sabe informar

( ) Outra técnica:_____

ANÁLISE DE RISCOS

O propósito desta etapa é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. Envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia.

11. Qual (is) técnica (s) sua instituição utiliza para análise de riscos relacionados à aquisição de TIC?

( ) Análise de Árvore de Decisões.

( ) Análise de Confiabilidade Humana.

( ) Estudo de Perigos e Operabilidade (HAZOP).

( ) Análise Preliminar de Riscos (APR)

( ) Checklist

( ) Técnica Estruturada de What If? (SWIFT).

( ) Não sabe informar

( ) Outra técnica:_____

AVALIAÇÃO DE RISCOS

O propósito da avaliação de riscos é apoiar decisões. Envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de: fazer mais nada, considerar as opções de tratamento de riscos, realizar análises adicionais para melhor compreender o risco, manter os controles existentes e reconsiderar os objetivos.

12. Qual (is) técnica (s) sua instituição utiliza para realizar avaliação de riscos relacionados à aquisição de TIC?

( ) Análise Crítica de Modos de Falha e Efeito.

( ) Técnica Estruturada de What If? (SWIFT).

( ) Simulação Monte Carlo.

( ) Análise de Causa Raiz.

( ) Matriz de Probabilidade / Impacto.

( ) Não sabe informar.

( ) Outra técnica: _____

TRATAMENTO DE RISCOS

O propósito desta etapa é selecionar e implementar opções para abordar riscos. Envolve um processo iterativo de formular e selecionar opções para tratamento do risco, planejar e implementar o tratamento de riscos, avaliar a eficácia deste tratamento, decidir se o risco remanescente é aceitável e se não for aceitável, realizar tratamento adicional. Você deve indicar mais de uma alternativa.

13. Na sua opinião, o que deve conter um plano de tratamento de riscos?

( ) Todos os riscos mapeados, probabilidade de ocorrência, dano potencial, consequência e ações de prevenção e ações de contingência.

( ) Ações que deverão ser desencadeadas, diante de adversidades, acidentes, sinistros, perda ou danos numa organização.

( ) Sequência de procedimentos necessários para fazer com que processos afetados voltem a funcionar.

( ) Não sabe informar.

( ) Outra opção: _____

MONITORAMENTO E CONTROLE

O propósito da etapa é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos.

14. Sua instituição realiza o monitoramento e controle de riscos em todas as fases da contratação?

( ) Sim ( ) Não ( ) Não sabe informar

15. Na sua opinião, como deve ser realizado o monitoramento e controle de riscos referente a gestão de riscos em aquisições de TIC?

( ) Através de checklists.

( ) Através de relatórios.

( ) Através de reuniões periódicas.

( ) Não sabe informar.

( ) Outra opção: _____

COMUNICAÇÃO E CONSULTA

Busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter o retorno e informação para auxiliar a tomada de decisão.

16. Como sua instituição realiza a comunicação sobre riscos no processo de contratação de TIC?

( ) Reuniões.

( ) Atas.

( ) Mapa de Gerenciamento de Riscos.

( ) Relatórios sumarizados.

( ) Lições aprendidas.

( ) Relatório Anual de Gestão.

( ) Não sabe informar

( ) Outra opção: _____

REGISTRO E RELATO

O registro e o relato visam: comunicar atividades e resultados de gestão de riscos em toda a organização, fornecer informações para a tomada de decisão, melhorar as atividades de gestão de riscos e auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos.

17. Quais ferramentas sua instituição utiliza para registrar os atos administrativos e lições aprendidas sobre a gestão de riscos no processo de aquisição de TIC?

( ) Planilha Eletrônica.

( ) Software Específico.

( ) Documento Eletrônico.

( ) Site Institucional.

( ) Pasta Compartilhada.

( ) Não sabe informar.

( ) Outra ferramenta:_____

SOLUÇÃO

18. Indique uma solução para a realização da gestão de riscos em aquisições de TIC?

( ) Guia

( ) Manual

( ) Metodologia

( ) Modelo

( ) Processo

( ) Outra solução:_____

19. Sugira uma ferramenta tecnológica para a realização da gestão de riscos em aquisições de TIC?

( ) Planilha Eletrônica

( ) Software

( ) Não sabe informar

( ) Outra ferramenta: _____

OPINIÃO DOS PARTICIPANTES

20. Sugira indicadores de desempenho para a gestão de riscos em aquisições de TIC.

_____

21. Indique sugestões de melhoria para a gestão de riscos em aquisições de TIC.

_____

22. Na sua opinião, quais são as dificuldades para uso de uma solução para a gestão de riscos no processo de aquisição de TIC?

---

23. Na sua opinião quais são as causas para a dificuldade em gerir riscos em aquisições de TIC?

_____

APÊNDICE E – ROTEIRO DE ENTREVISTA

ENTREVISTA SOBRE GESTÃO DE RISCOS EM AQUISIÇÕES DE TIC

A. Identificação do Entrevistado

1. Qual é a instituição que você trabalha? _____

B. Área de atuação

2. Qual é a sua área de atuação?

_____

C. Gestão de Riscos

3. Como sua instituição realiza a gestão de riscos em aquisições de TIC?

_____

4. Na sua opinião, como a gestão de riscos deve ser realizado em aquisições de TIC?

_____

5. Que atividades você sugere para a gestão de riscos em aquisições de TIC?

_____

6. Na sua opinião qual é a solução ideal para a gestão de riscos em aquisições de TIC?

_____

7. Na sua opinião, quais são as barreiras que dificultam a realização da gestão de riscos em aquisições de TIC?

( ) Falta de apoio da gestão ( ) Cultura organizacional ( ) Comunicação fraca ( ) Inexistência de capacitações ( ) Outra:_____

8. Na sua opinião, quais são as variáveis facilitadoras para a gestão de riscos em aquisições de TIC?

( ) Planejamento das atividades ( ) Padronização de documentos

( ) Sistematização de rotinas de trabalho ( ) Transparência de Informações

( ) Outra: _____

APÊNDICE F – PERFIL DE ENTREVISTADOS

(Adaptado da Instrução Normativa Nº1/2019 de 4 de abril de 2019)

N	Perfil	Papel	Responsabilidade
E1	Trabalha na Instituição há 15 anos. Já participou de vários processos de aquisição de TIC tanto como integrante requisitante, técnico e fiscal técnico do contrato.	Gerente de TIC Analista de TIC Integrante Requisitante	- Construir o Documento de Oficialização de Demanda
E2	Trabalha na Instituição há 10 anos. Já participou de vários processos de aquisição de TIC em órgãos estaduais e federais. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Diretor de TIC Coordenação de TIC Analista de TIC Integrante Técnico	- Instruir processo de aquisição de TIC - Solicitar recursos financeiros para a aquisição - Conduzir o trabalho da equipe de planejamento da aquisição
E3	Trabalha na Instituição há 7 anos. Já participou de vários processos de aquisição de TIC em órgãos estaduais e federais. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Coordenação de TIC Analista de TIC Integrante Técnico	- Realizar pesquisa de mercado - Criar do Estudo Técnico Preliminar - Construir o Termo de Referência - Analisar Riscos - Avaliar propostas de orçamento
E4	Trabalha na Instituição há 5 anos. Já participou de vários processos de aquisição de TIC em órgãos estaduais e federais. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Coordenação de TIC Analista de TIC Fiscal Administrativo do contrato	- Fiscalizar o contrato do ponto de vista técnico
E5	Trabalha na Instituição há 12 anos. Já participou de vários processos de aquisição de TIC em órgãos federais. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Pregoeiro	- Conduzir o trabalho da equipe de apoio - Construir o Edital - Construir a minuta do contrato - Habilitar / Inabilitar fornecedores - Conduzir o processo licitatório - Julgar recursos - Adjucar e homologar o resultado da licitação - Indicar vencedor do certame
E6	Trabalha na Instituição há 12 anos. Já participou de vários processos de aquisição de TIC em órgãos federais. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Fiscal Administrativo do Contrato	- Divulgar avisos sobre a aquisição - Fiscalizar o contrato do ponto de vista administrativo - Avaliar propostas - Avaliar questionamentos do ponto de vista administrativo - Avaliar impugnações do ponto de vista administrativo
E7	Trabalha na Instituição há 8 anos. Já participou de vários processos de aquisição de TIC na Instituição. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC.	Diretor de Administração Integrante Administrativo	- Empenhar recursos financeiros para a aquisição - Pagar de fornecedores
E8	Trabalha na Instituição há 5 anos. Já participou de vários processos de aquisição de TIC na Instituição. Possui capacitação na legislação vigente sobre contratações de TIC. Faz parte da atual equipe de planejamento da contratação de TIC	Gestor de Contrato Integrante Administrativo	- Celebrar contrato - Aplicar sanções administrativas para o processo de aquisição - Encerrar o Contrato

APÊNDICE G – ROTEIRO DE AVALIAÇÃO DA SOLUÇÃO

Objetivo: coletar informações sobre o uso da metodologia GRATIC em um contexto real.

Público Alvo: servidores públicos que participam ou já participaram da equipe de planejamento de aquisições de TIC.

1. A solução apresentada é capaz de executar as atividades definidas para realizar a gestão de riscos em aquisições de TIC?

( ) Discordo Totalmente

( ) Discordo Parcialmente

( ) Indiferente

( ) Concordo Parcialmente

( ) Concordo Totalmente

2. A solução apresentada contribui para que a gestão de riscos em aquisições de TIC seja realizada no tempo previsto?

( ) Discordo Totalmente

( ) Discordo Parcialmente

( ) Indiferente

( ) Concordo Parcialmente

( ) Concordo Totalmente

3. A solução apresentada pode ser utilizada para outro tipo de aquisição?

( ) Discordo Totalmente

( ) Discordo Parcialmente

( ) Indiferente

( ) Concordo Parcialmente

( ) Concordo Totalmente

4. A solução apresentada é de fácil compreensão e uso?

( ) Discordo Totalmente

( ) Discordo Parcialmente

( ) Indiferente

( ) Concordo Parcialmente

( ) Concordo Totalmente

5. Faça uma avaliação crítica sobre a solução proposta?

_____

6. O que sugere para melhorar a solução proposta?

_____

APÊNDICE H – ARTEFATOS DA METODOLOGIA GRATIC

Artefato	Endereço Eletrônico
Planilha Documentadora	https://docs.google.com/spreadsheets/d/10WeCVJGX4vJqaZe72sc6Ae6p1-YlplM5/edit#gid=750989905
Repositório Digital de Informações	https://sites.google.com/a/cin.ufpe.br/riskitcbr/
Manual da Metodologia	https://docs.google.com/document/d/1cqcVu-m4JtgwKPSc5VvX-0PG3jxRU0Of7gQWz00Lig0/edit

APÊNDICE I – CHECKLIST: FONTES DE RISCO

(adaptado de Silva, 2014 e Nobre, 2017)

Data:	
Participantes:	

Fonte de Risco	Descrição	Resposta	Status
Áreas de negócio	A aquisição está alinhada com PDTI?	Sim	OK
	A aquisição está no Plano Anual de Contratações?	Sim	OK
	A aquisição está alinhada com PDTI?	Sim	OK
	A aquisição de TIC está ligada a algum objetivo estratégico?	Sim	OK
	A demanda foi solicitada informando modelo ou marca?	Sim	OK
	Existe conhecimento do projeto na alta administração?	Sim	OK
Processos	Existe processo devidamente formalizado para aquisição de TIC?	Sim	OK
	A solução a ser contratada exige mudança de cultura da organização?	Sim	OK
	Existe um levantamento da real necessidade de aquisição de TIC?	Sim	OK
	Os requisitos técnicos da aquisição são bem definidas?	Sim	OK
	Há uma justificativa para previsão de quantidade dos itens da solução de TI?	Sim	OK
Recursos Humanos	A Equipe de planejamento tem perfil adequado para condução do processo de contratação de TI	Não	Cuidado
	Existe quantidade suficiente de pessoal para suportar a demanda de aquisições em TI?	Não	Alerta
	Existe comunicação e interação entre os membros da equipe de aquisição?	Não	Alerta
	Os servidores indicados para equipe de planejamento dispõem de tempo para as atribuições de planejamento da aquisição?	Não	Alerta
Recursos Financeiros	Existe orçamento designado para aquisição de TI?	Não	Cuidado

	Existe sobra de produtos ou serviços, levando ao desperdício de recursos financeiros?	Não	OK
	Há uma análise de custo benefício para a aquisição a ser realizada:	Não	Alerta
	Existe coleta concisa de cotação de preços?	Sim	OK
	O preço da solução está dentro da média de mercado?	Sim	OK
Legislação	Existe análise jurídica por área competente?	Sim	OK
	A aquisição tem legislação própria que o controle?	Sim	OK
	A especificação técnica atende a vários fornecedores?	Sim	OK
	A solução de TI está parcelada	Sim	OK
Qualidade	Os requisitos técnicos são específicos de uma marca/modelo?	Não	Alerta
	Existe risco da solução atender apenas parcialmente a instituição	Sim	OK
	A solução é madura ou pode levar a descontinuidade antes da instituição desfrutar do investimento?	Sim	OK
Tecnologia	A solução é de padrão proprietário?	Não	OK
	A solução é obsoleta ou está próxima de ser tornar obsoleta, o que levaria à descontinuidade antes da instituição desfrutar do investimento?	Não	OK
	Existe necessidade de aquisição de outra solução de TI para que a solução a ser contratada funcione corretamente?	Não	OK
	Existe dificuldade para elaboração da especificação técnica?	Sim	Cuidado
Tempo	Pode ocorrer atraso no alcance dos resultados pretendidos com a contratação devido alguma intempestividade ou adequação da instituição?	Não	Alerta
	Pode ocorrer atraso no início dos trabalhos devido a contratada não possuir condições necessárias para a execução?	Não	Alerta
	Pode ocorrer atraso na finalização da aquisição, paralisando algum serviço essencial da Instituição?	Sim	Cuidado

APÊNDICE J – INVENTÁRIO DE RISCOS

PLANILHA DE IDENTIFICAÇÃO DE RISCOS

INVENTÁRIO DE RISCOS

Nº	DESCRIÇÃO DO RISCO	PROPRIETÁRIO DO RISCO	CAUSA DO RISCO	EFEITO/DANO/CONSEQUÊNCIA	CATEGORIA	FASE DA CONTRATAÇÃO
1	Ausência da formalização da demanda que originou a contratação	Área requisitante	Falta de normativa interna para formalização de demandas	Contratação que não atende à necessidade que originou a demanda	Conformidade	Planejamento da Contratação
2	Descrição imprecisa da demanda	Área requisitante	Especificação inconsistente da demanda	Contratação e execução dificiente do objeto	Conformidade	Planejamento da Contratação
3	Falta de clareza na definição de requisitos técnicos	Área requisitante	Falta de compreensão da necessidade	Contratação de solução que não atende à necessidade que originou a contratação.	Conformidade	Planejamento da Contratação
4	Definição de requisitos técnicos que limitam a ampla concorrência vedando a participação de alguns fornecedores	Área de TI	Falta de compreensão das normativas vigentes	Limitação indevida da competição.	Conformidade	Planejamento da Contratação
5	Estimativa de quantidade menor que as necessidades das instituição	Área requisitante	Desconhecimento da necessidade	Não atendimento das necessidades que foram demandadas	Operacional	Planejamento da Contratação
6	Ausência de ato de designação da equipe de planejamento de contratação	Alta Gestão	Não observação da legislação vigente sobre contratações	Descumprimento de formalidade legal	Conformidade	Planejamento da Contratação
7	Indefinição de papéis e responsabilidades da equipe de planejamento de contratação	Alta Gestão	Inobservância de normativas vigentes	Sobrecarga de trabalho para alguns membros da equipe	Estratégico	Planejamento da Contratação
8	Equipe de planejamento da contratação de TI não detém as competências multidisciplinares necessárias à execução da atividade	Alta Gestão	Inexistência de cursos de capacitação continuada	Erros na tramitação do processo licitatório	Estratégico	Planejamento da Contratação
9	Falta de integração da equipe de planejamento da contratação	Equipe de Planejamento da Contratação	Inexistência de reuniões periódicas	Erros na instrução do processo licitatório	Estratégico	Planejamento da Contratação
10	Decisões sobre as aquisições dispersas na organização	Equipe de Planejamento da Contratação	Falta de comunicação entre os setores da organização	Ausência de priorização das aquisições que apoiam a implementação das ações organizacionais mais relevantes.	Operacional	Planejamento da Contratação

APÊNDICE K – AVALIAÇÃO DE PROBABILIDADE

PLANILHA DE AVALIAÇÃO DE PROBABILIDADE

AVALIAÇÃO DE PROBABILIDADE RISCOS

LEGENDA DE CLASSIFICAÇÃO DE PROBABILIDADE

Elevada	
Muito alta	
Alta	
Média	
Baixa	

Tipo de Controle	Nível	%
Corretivo	Inexistente	>75
	Fraco	<=75
Detectivo	Insatisfatório	<=60
Preventivo	Satisfatóro	<=40
	Forte	<=20

Fatores de Risco	
5 - Elevado	
4 - Muito Alta	
3 - Alto	
3 - Médio	
1 - Baixa	

Nº	RISCOS	CONTROLES EXISTENTES			ESTRUTURA ANALÍTICA DE RISCOS									CLASSIFICAÇÃO PROBABILIDADE	PROBABILIDADE (%)
		MEDIDA DE CONTROLE	TIPO DE CONTROLE EXISTENTE	MATURIDADE	TI	RH	PRO	ORG	LEG	COM	FR	ER	GP		
1	Ausência da formalização da demanda que originou a contratação	Lista de Verificação	Corretivo	Insatisfatório	1	1	5	5	5	5	3.67	5	18.33	Muito Alta	73.33
2	Descrição imprecisa da demanda	Lista de Verificação	Corretivo	Insatisfatório	1	1	4	4	4	4	3.00	5	15.00	Alta	60.00
3	Falta de clareza na definição de requisitos técnicos	Lista de Verificação	Corretivo	Inexistente	1	5	5	5	5	5	4.33	5	21.67	Elevada	86.67
4	Definição de requisitos técnicos que limitam a ampla concorrência vedando a participação de alguns fornecedores	Estudo Técnico Preliminar	Preventivo	Fraco	2	3	4	5	5	5	4.00	4	16.00	Muito Alta	64.00
5	Estimativa de quantidade menor que as necessidades das instituição	Pesquisa de mercado	Preventivo	Fraco	3	3	3	4	1	1	2.50	5	12.50	Alta	50.00
6	Ausência de ato de designação da equipe de planejamento de contratação	Lista de Verificação	Corretivo	Satisfatório	3	3	2	2	1	1	2.00	5	10.00	Média	40.00
7	Indefinição de papéis e responsabilidades da equipe de planejamento de contratação	Lista de Verificação	Preventivo	Satisfatório	2	2	4	2	2	2	2.33	4	9.33	Média	37.33
8	Equipe de planejamento da contratação de TI não detém as competências multidisciplinares necessárias à execução da atividade	Capacitação	Preventivo	Satisfatório	2	3	3	2	4	4	3.00	3	9.00	Média	36.00
9	Falta de integração da equipe de planejamento da contratação	Plano de Comunicação	Preventivo	Insatisfatório	5	4	4	4	4	4	4.17	5	20.83	Elevada	83.33
10	Decisões sobre as aquisições dispersas na organização	Reuniões periódicas	Detectivo	Insatisfatório	5	5	5	5	3	4	4.50	5	22.50	Elevada	90.00

APÊNDICE L – AVALIAÇÃO DE IMPACTO

PLANILHA DE AVALIAÇÃO DE IMPACTO

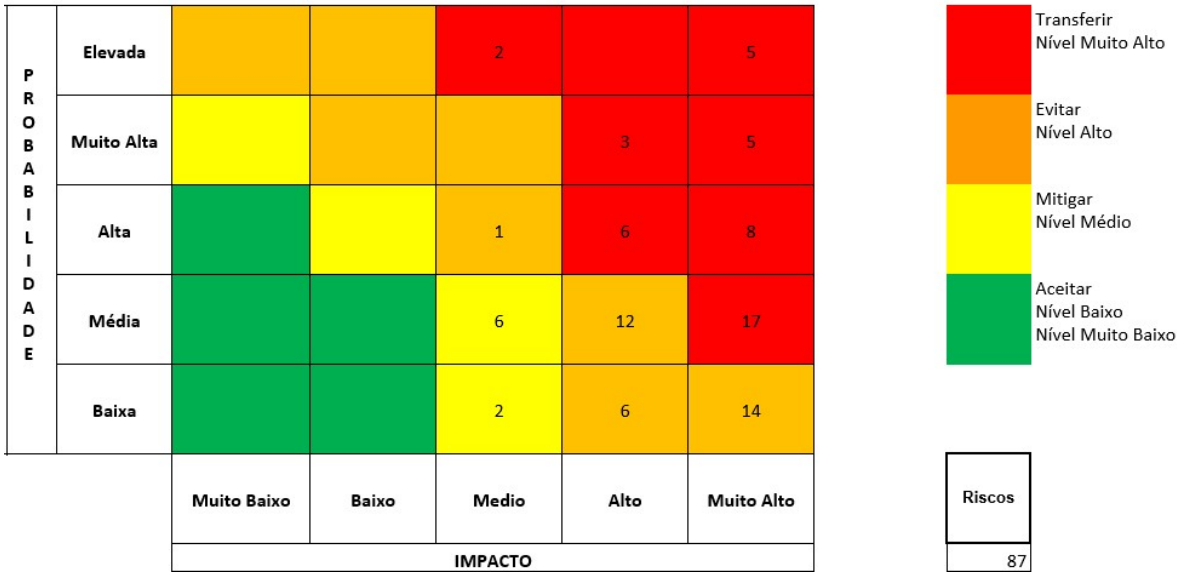
AVALIAÇÃO DE IMPACTO DOS RISCOS

LEGENDA DE NÍVEL DE IMPACTO

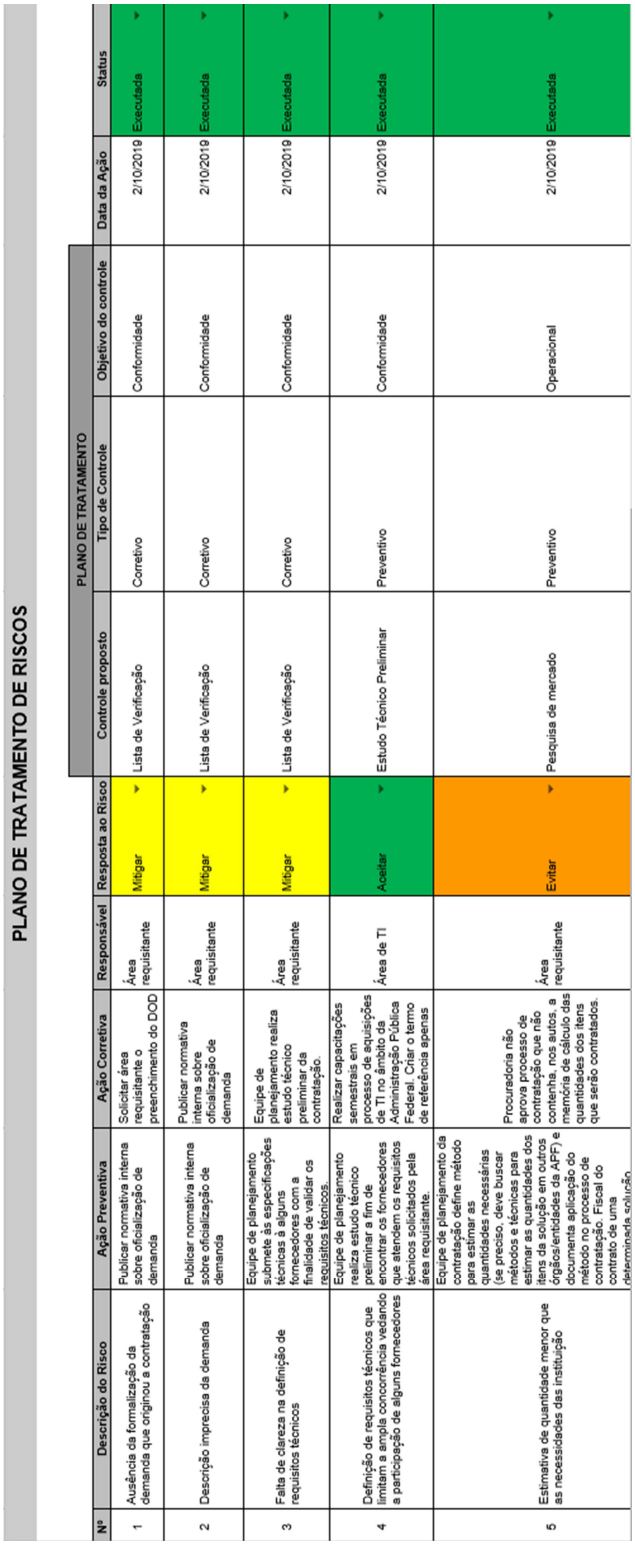
Muito Alto	5
Alto	4
Médio	3
Baixo	2
Muito Baixo	1

Nº	RISCOS	IMAGEM	FINANCEIRO	LEGISLAÇÃO	OPERACIONAL	MÉDIA DO IMPACTO	NÍVEL DE IMPACTO
1	Ausência da formalização da demanda que originou a contratação	5	2	5	5	4.25	Alto
2	Descrição imprecisa da demanda	4	4	5	5	4.50	Alto
3	Falta de clareza na definição de requisitos técnicos	5	5	5	5	5.00	Muito alto
4	Definição de requisitos técnicos que limitam a ampla concorrência vedando a participação de alguns fornecedores	5	3	5	4	4.25	Alto
5	Estimativa de quantidade menor que as necessidades das instituição	2	5	3	5	3.75	Alto
6	Ausência de ato de designação da equipe de planejamento de contratação	2	2	4	5	3.25	Medio
7	Indefinição de papéis e responsabilidades da equipe de planejamento de contratação	3	3	4	4	3.50	Medio
8	Equipe de planejamento da contratação de TI não detém as competências multidisciplinares necessárias à execução da atividade	3	4	5	5	4.25	Alto
9	Falta de integração da equipe de planejamento da contratação	3	3	3	5	3.50	Medio
10	Decisões sobre as aquisições dispersas na organização	4	3	3	4	3.50	Medio

APÊNDICE M – MATRIZ DE PROBABILIDADE E IMPACTO



APÊNDICE N – PLANO DE TRATAMENTO DE RISCOS



PLANO DE TRATAMENTO DE RISCOS

Nº	Descrição do Risco	Ação Preventiva	Ação Corretiva	Responsável	Resposta ao Risco	PLANO DE TRATAMENTO			Data da Ação	Status
						Controle proposto	Tipo de Controle	Objetivo do controle		
1	Ausência da formalização da demanda que originou a contratação	Publicar normativa interna sobre oficialização de demanda	Solicitar área requisitante o preenchimento do DOD	Área requisitante	Mitigar	Lista de Verificação	Corretivo	Conformidade	2/10/2019	Executada
2	Descrição imprecisa da demanda	Publicar normativa interna sobre oficialização de demanda	Publicar normativa interna sobre oficialização de demanda	Área requisitante	Mitigar	Lista de Verificação	Corretivo	Conformidade	2/10/2019	Executada
3	Falta de clareza na definição de requisitos técnicos	Equipe de planejamento submete às especificações técnicas a alguns fornecedores com a finalidade de validar os requisitos técnicos.	Equipe de planejamento realiza estudo técnico preliminar da contratação.	Área requisitante	Mitigar	Lista de Verificação	Corretivo	Conformidade	2/10/2019	Executada
4	Definição de requisitos técnicos que limitam a ampla concorrência vedando a participação de alguns fornecedores	Equipe de planejamento realiza estudo técnico preliminar a fim de encontrar os fornecedores que atendem os requisitos técnicos solicitados pela área requisitante.	Realizar capacitações semestrais em processo de aquisições de TI no âmbito da Administração Pública Federal. Criar o termo de referência apenas	Área de TI	Aceitar	Estudo Técnico Preliminar	Preventivo	Conformidade	2/10/2019	Executada
5	Estimativa de quantidade menor que as necessidades das instituição	Equipe de planejamento da contratação define método para estimar as quantidades necessárias (se preciso, deve buscar métodos e técnicas para estimar as quantidades dos itens da solução em outros órgãos/entidades da APF) e documenta aplicação do método no processo de contratação. Fiscal do contrato de uma determinada solução	Procuradoria não aprova processo de contratação que não contenha, nos autos, a memória de cálculo das quantidades dos itens que serão contratados.	Área requisitante	Evitar	Pesquisa de mercado	Preventivo	Operacional	2/10/2019	Executada

APÊNDICE O – MONITORAMENTO E CONTROLE

MONITORAMENTO E CONTROLE DA EXECUÇÃO DE FASES DA AQUISIÇÃO DE TIC

Processo nº

Tipo:

Modalidade:

PLANEJAMENTO DA CONTRATAÇÃO					
ATOS ADMINISTRATIVOS E DOCUMENTOS A SEREM VERIFICADOS	**Situação**	**Responsável**	**Publicado**	**Observação**	**Data**
1. Abertura de processo administrativo devidamente autuado, protocolado e numerado (art. 38, caput, da Lei nº 8.666/93), ou registrado quando processo eletrônico?	Não iniciado		Sim		
2. Consta a solicitação/requisição do objeto (DOD), elaborada pelo agente ou setor competente assinada pela autoridade competente da unidade (Acórdão 254/2004-Segunda Câmara-TCU)?	Não iniciado		Sim		
2.1. A autoridade competente da unidade demandante definiu o objeto do certame de forma precisa, suficiente e clara e é compatível com o objeto da pesquisa de preços, sem direcionamento de marca ou fornecedor?	Não iniciado		Sim		
2.1.1. Consta dos autos a requisição da contratação (compra) no Plano Anual de Contratações de TI?	Não iniciado		Sim		
2.1.2. Consta dos autos a requisição da contratação (compra) no PDTI?	Não iniciado		Sim		
3. Consta a Portaria de Designação da Equipe de Planejamento da Contratação?	Não iniciado		Sim		

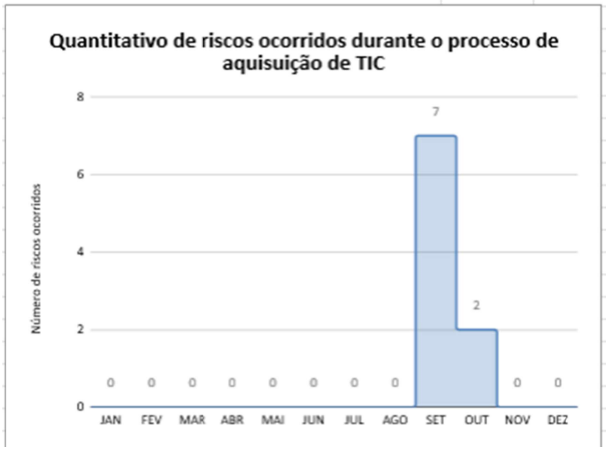
APÊNDICE P – RELATÓRIO EVOLUTIVO DE RISCOS

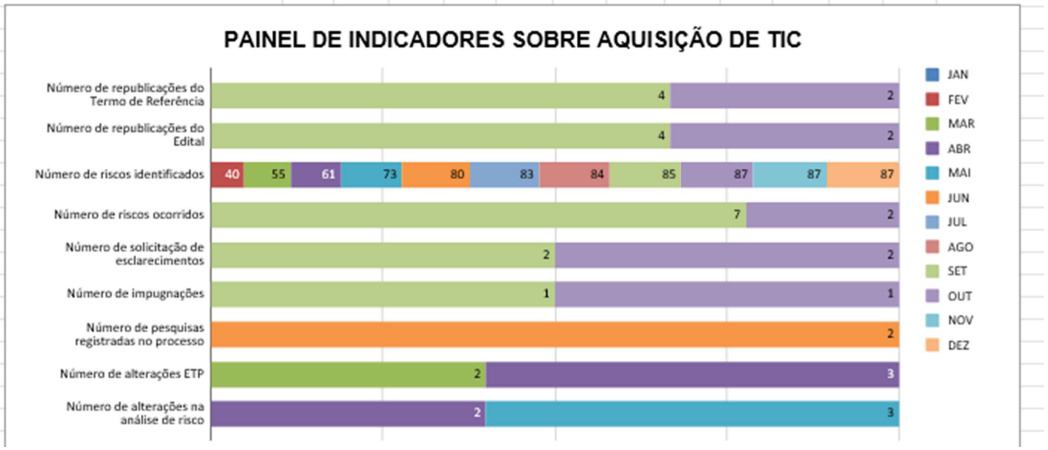
RELATÓRIO EVOLUTIVO DE RISCOS

Risco ocorrido	Responsável pela correção	Frequência	Houve Mudanças no processo	Ações corretivas	Lições aprendidas	Data
Ausência da formalização da demanda que originou a contratação	Fernando Torres	Por evento	Não	Área Técnica criou o documento	Exigir o DOD do setor requisitante. Caso não tenha oo responsável pela área administrativa deverá assinar o documento.	02/10/2019
Falta de clareza na definição de requisitos técnicos	Maria Teresa	Por evento	Sim	Correção do Termo de Referência e Edital	Revisar o Termo de Referência e Edital por pelo menos dois membros da equipe de planejamento antes da publicação, sendo um membro da área técnica e outro da área administrativa.	02/10/2019
Definição de requisitos técnicos que limitam a ampla concorrência vedando a participação de alguns fornecedores	Carlos Patrocinio	Aleatório	Sim	Correção do Termo de Referência	Levar em consideração os apontamentos feitos na pesquisa de mercado	02/10/2019
Equipe de planejamento da contratação de TI não detém as competências multidisciplinares necessárias à execução da atividade	Danilo Custódio	Aleatório	Sim	Plano de Capacitação	Realizar capacitação periódica	02/10/2019
Falta de integração da equipe de planejamento da contratação	Patricia Nolasco	Aleatório	Sim	Plano de Comunicação	Realizar reuniões periódicas de acompanhamento e revisão de artefatos	02/10/2019
Responsável pela seleção do fornecedor (tipicamente o pregoeiro) não detém as competências multidisciplinares necessárias à execução da atividade (e.g., conhecimentos técnicos do objeto, conhecimentos jurídicos aprofundados).	Pedro Henrique	Aleatório	Sim	Plano de Capacitação	Realizar capacitação periódica	02/10/2019
Direcionamento de marca ou fabricação	Tatiana Paniago	Aleatório	Sim	Plano de Capacitação	Levar em consideração os apontamentos feitos na pesquisa de mercado	02/10/2019

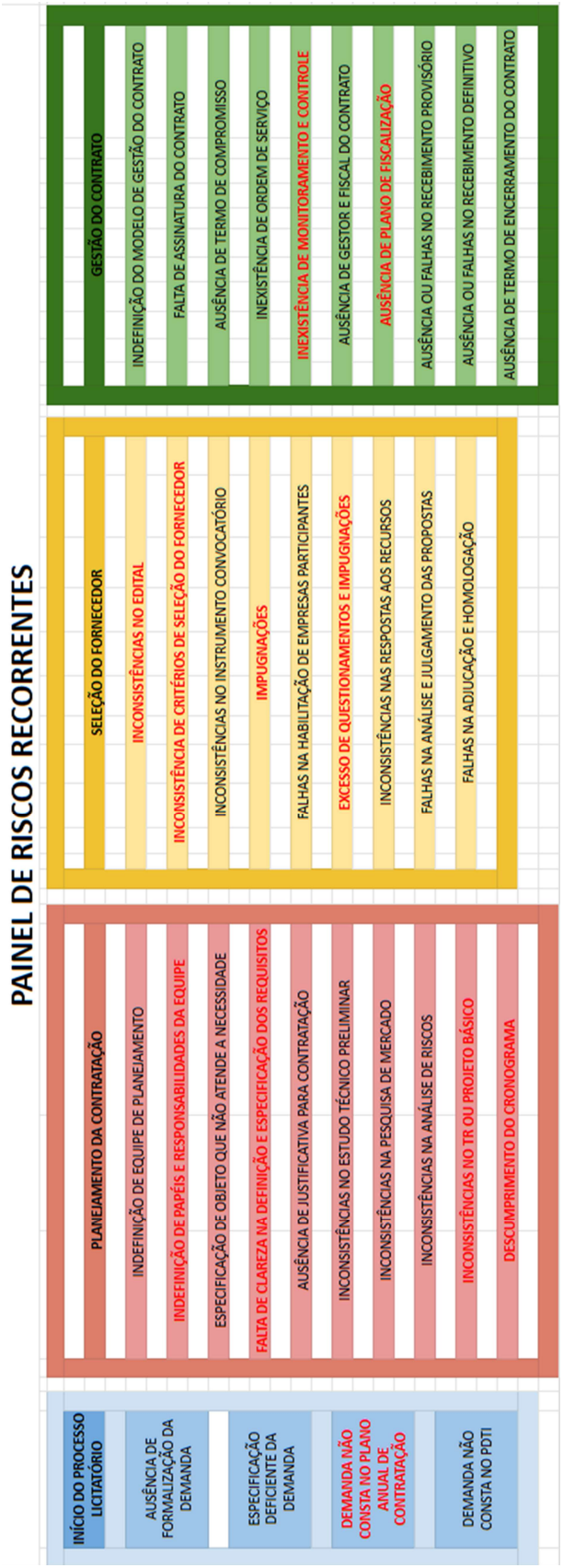
PAINEL DE INDICADORES PARA CONTROLE DE RISCOS EM AQUISIÇÕES DE TIC

			2019											
Indicador	**Métrica**	Fórmula	JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ	**TOTAL**
Quantidade de republicações do Termo de Referência	Crescente	Número de republicações do Termo de Referência									4	2			6
Quantidade de republicações do Edital	Crescente	Número de republicações do Edital									4	2			6
Quantidade de riscos identificados	Crescente	Número de riscos identificados	0	40	55	61	73	80	83	84	85	87	87	87	84
Quantidade de riscos ocorridos	Crescente	Número de riscos ocorridos									7	2			9
Quantidade esclarecimentos	Crescente	Número de solicitação de esclarecimentos									2	2			4
Quantidade de impugnações	Crescente	Número de impugnações									1	1			2
Quantidade de alterações na pesquisa de mercado	Crescente	Número de pesquisas registradas no processo						2							2
Quantidade de alterações no estudo técnico preliminar	Crescente	Número de alterações ETP			2	3									5
Quantidade de alterações na análise de riscos	Crescente	Número de alterações na análise de risco				2	3								5





APÊNDICE R - PAINEL DE RISCOS



APÊNDICE S – PLANO DE COMUNICAÇÃO

PLANO DE COMUNICAÇÃO						
Stakeholder (Who?)	**Propósito (Why?)**	**O que e como / Ferramenta (What e How?)**	**Responsável (Who 2?)**	**Quando (data) / Frequência (When?)**	**Onde acessar / Armazenar (Where?)**	**Custo (How much?)**
Equipe de Planejamento de Aquisição de TIC	Informar os riscos ocorridos em cada fase do processo de aquisição	Reunião de planejamento da aquisição e ata de reunião via e-mail	Integrante Administrativo	Encerramento da fase do processo de aquisição	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Apresentar Estudo Técnico Preliminar	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Técnico	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Apresentar relatório de gestão de risco em cada fase do processo de aquisição de TIC	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Técnico	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Divulgar Termo de Referência	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Técnico	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Publicar Edital	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações Publicar no site institucional Publicar no site compras governamentais	Integrante Administrativo	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Encaminhar questionamentos sobre Termo de Referência	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Administrativo	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Equipe de Planejamento de Aquisição de TIC	Encaminhar impugnações sobre Termo de Referência	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Administrativo	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Partipante da licitação	Responder questionamentos sobre Termo de Referência	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações Publicar no site de compras governamentais	Integrante Técnico	Até 2 dias após receber notificação	Sistema Eletrônico de Informações	2 horas
Partipante da licitação	Responder impugnações sobre Termo de Referência	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações Publicar no site de compras governamentais	Integrante Técnico	Até 2 dias após receber notificação	Sistema Eletrônico de Informações	2 horas
Integrante Administrativo	Publicar Contrato	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Integrante Administrativo	Finalização da construção do documento	Sistema Eletrônico de Informações	2 horas
Fornecedor	Informar início do contrato	"Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações Publicar no site institucional	Gestor do Contrato	Início da execução do contrato	Sistema Eletrônico de Informações	2 horas
Fornecedor	Informar não cumprimento do contrato	Encaminhar por e-mail Publicar no Sistema Eletrônico de Informações	Fiscal Técnico	Execução do Contrato	Sistema Eletrônico de Informações	2 horas