Gestão de Riscos nas Aquisições de Soluções de TI: Uma Análise Crítica dos Modelos de Boas Práticas

Tatieures G. Pires[1], Sueli M. de A. Cavalcante[2], Denise M. M. C. Corrêa[2], Joaquim B. C. Neto[3]

[1]Auditoria Geral - Universidade Federal do Ceará - Fortaleza, CE - Brasil

[2]Pró-Reitoria de Administração - Universidade Federal do Ceará - Fortaleza, CE - Brasil

[3]Secretaria de Tecnologia da Informação - Universidade Federal do Ceará - Fortaleza, CE - Brasil

tatieures@ufc.br, {sueli,pradm}@pradm.ufc.br, joaquim.bento@sti.ufc.br

Abstract. *IT Acquisitions represents an important strategic role in organizations and move a large volume of financial resources. Due to the complexity of the IT environment, these acquisitions are constantly subject to risk factors with high likelihood and impact. In Brazilian Federal Public Administration, these acquisitions are directed by specific process, defined by Normative Instruction n. 04/2014, in order to minimize potential failures. However, this flow does not emphasize risk management. The objective of this research is to identify the main models of best practices in risk management consistent with the public IT Acquisitions, in order to encourage this practice in Public Administration.*

Resumo. *As contratações de TI assumem importante função estratégica nas organizações e movimentam um grande volume de recursos financeiros. Devido à complexidade inerente ao ambiente de TI, essas contratações estão constantemente sujeitas a fatores de riscos de alta probabilidade e impacto. Na Administração Pública Federal brasileira, essas aquisições são disciplinadas por processo específico, definido pela Instrução Normativa nº 04/2014, com o intuito de minimizar possíveis falhas. No entanto, esse fluxo não enfatiza a gestão de riscos. O objetivo desta pesquisa é identificar os principais modelos de boas práticas em gestão de riscos compatíveis com as contratações públicas de TI, no sentido de fomentar essa prática na Administração Pública.*

1. Introdução

As aquisições de tecnologia da informação (TI) na Administração Pública, de maneira geral, costumam ser bastante complexas, exigindo da equipe de contratação que disponha de conhecimento técnico aprofundado no assunto, além de competências para planejar e gerir adequadamente a aquisição, de acordo com a legislação vigente.

Apesar do aporte legal, que subsidia esse processo, é comum haver, nessas contratações, discrepância entre o que foi planejado e a efetiva execução do contrato. Isso ocorre porque algumas condições envolvidas na contratação são difíceis de quantificar e gerenciar, como, por exemplo, o equilíbrio entre prazo, custo e qualidade, a gestão de mudanças, a forma de aceitação, a transferência de conhecimentos, etc. Essas incertezas geram riscos para ambas as partes, contratado e contratante, e podem levar a sérios conflitos durante a execução contratual [SOFTEX 2013].

Para o Tribunal de Contas da União (TCU), os riscos em projetos de TI "chegam a ser prováveis em muitos casos, como o aumento dos custos inicialmente previstos e a dilação do prazo de entrega do produto. Não raro, o projeto fracassa no alcance de seus objetivos, e compromete ações institucionais" [BRASIL 2012].

A necessidade de gerir riscos já tem sido reportada pelo TCU, mesmo que de forma genérica. No relatório do último Levantamento de Governança de TI ele constatou que as organizações públicas federais ainda não reconhecem a importância da gestão de riscos, apesar do volume de recursos geridos e riscos aos quais estão expostas e atribui à Alta Administração dos órgãos a responsabilidade por viabilizar e manter o funcionamento adequado de mecanismos de gestão de riscos [BRASIL 2014b].

Normalmente a gestão de riscos é vista como um processo complexo, difícil de ser implantando e executado. De fato, para que ela seja efetiva, é preciso estabelecer uma cultura institucional orientada a riscos e prover infraestrutura adequada, baseada em uma metodologia sistemática e confiável, e isso não constitui uma tarefa fácil.

Uma grande dificuldade enfrentada pelas instituições quando desejam implantar mecanismos para gerir riscos é a necessidade de avaliar os diversos *frameworks* existentes para verificar a sua aderência ao contexto organizacional. Esse trabalho exige bastante tempo e paciência, recursos muitas vezes escassos nos ambientes corporativos.

No entanto, a não realização desse levantamento para definir a abordagem a ser seguida inviabiliza a gestão de riscos, devido à dificuldade de estabelecer um dialeto comum entre as partes envolvidas. Se cada participante carregar consigo conhecimento sobre uma técnica distinta é improvável que se consiga estabelecer integração entre os participantes pela ausência de padronização.

No caso das instituições públicas, esse problema é ainda mais evidente, tendo em vista a pequena quantidade de estudos práticos realizados que verifiquem a aplicabilidade de *frameworks* de mercado à sua realidade.

Diante do exposto, surge o seguinte questionamento: quais os principais modelos de gestão de riscos adotados no mercado brasileiro, aplicáveis ao contexto das contratações públicas de tecnologia da informação?

Portanto, o objetivo geral desta pesquisa é analisar a adequabilidade dos modelos de boas práticas em gestão de riscos difundidos no mercado e na academia às contratações públicas de TI, identificando os principais frameworks compatíveis com esse contexto. Nesse sentido, é preciso conhecer profundamente as abordagens mencionadas e extrair, de cada uma delas, as práticas mais adequadas para esse cenário, que possam ser implantadas, em conformidade com a legislação e com a jurisprudência dos órgãos de controle.

2. Metodologia

A partir dos objetivos traçados, a proposta metodológica deste trabalho tem o intuito de gerar conhecimento para posterior aplicação prática, baseada em abordagem exploratória e qualitativa.

Segundo Prodanov e Freitas (2013), a pesquisa exploratória "tem como finalidade proporcionar mais informações" acerca do assunto estudado. Através dela é possível definir e delimitar o tema da pesquisa, fixar os objetivos e formular hipóteses para o assunto. No presente estudo, essa abordagem foi utilizada para compreender o cenário atual da gestão de riscos no setor público, especialmente no que tange às contratações de tecnologia da informação, e explorar os modelos comumente adotados

na iniciativa privada, bem como trabalhos científicos nessa área.

Este estudo consiste na pesquisa e análise documental relativa às contratações de TI (normativos, jurisprudência, relatórios de auditoria, etc.) e pesquisa bibliográfica em trabalhos acadêmicos, artigos científicos, livros e modelos de referência em contratações de TI, engenharia de software, gerência de projetos e gestão de riscos.

Do ponto de vista da abordagem qualitativa, este trabalho busca selecionar os modelos de boas práticas atualmente adotados no mercado mais apropriados ao escopo da pesquisa, a partir da análise do contexto das contratações públicas de TI.

Cumpre ressaltar o caráter científico da pesquisa, considerando a análise criteriosa de práticas utilizadas em outros contextos em um novo panorama, através de estudo sistemático e fundamentado, ampliando o alcance desse conhecimento.

3. Contratações de TI na Administração Pública Federal

No âmbito no Poder Executivo Federal, os procedimentos administrativos devem ser estritamente orientados pela legislação vigente. No caso das aquisições de TI, além da legislação aplicável a todas as contratações públicas, esse processo é regido, em particular, pela Instrução Normativa nº 04/2014.

Os trâmites dispostos nesse normativo apresentam procedimentos específicos de planejamento, seleção do fornecedor e gerenciamento da execução para esse tipo de contratação, sendo consentida a sua adequação à estrutura funcional da instituição.

Além da legislação, deve-se observar ainda as deliberações do TCU. Compreende-se que a jurisprudência correlata às contratações de TI foi em grande parte incorporada à Instrução Normativa nº 04/2014 pela SLTI.

Para execução deste trabalho, realizou-se, além da pesquisa na legislação vigente, levantamento das decisões mais relevantes nesse tema. Dentre eles, destacaram-se as notas técnicas da Secretaria de Fiscalização de TI, que tratam do entendimento do TCU em assuntos específicos nas contratações de TI e os acórdãos nº 2.471/2008-TCU-Plenário, 2.535/2012–TCU–Plenário, 2.314/2013-TCU-Plenário e 916/2015-TCU-Plenário que consolidam os resultados das auditorias e fiscalizações realizadas, bem como recomendações de melhoria propostas pelo Tribunal.

Observou-se que a Instrução Normativa nº 04/2014 menciona a obrigatoriedade de realizar levantamento e avaliação dos riscos nas contratações, incluindo a definição de ações preventivas e contingenciais e seus respectivos responsáveis. No entanto, não existem, no âmbito da Administração Pública, instrumentos que definam expressamente as diretrizes para realizar gestão de riscos, considerando as peculiaridades das contratações públicas.

4. Gestão de Riscos

De acordo com a Associação Brasileira de Normas Técnicas (ABNT) (2009), risco pode ser definido como o "efeito da incerteza nos objetivos", um desvio (positivo ou negativo), em relação ao esperado.

Invariavelmente, qualquer objetivo traçado, seja na esfera pessoal ou profissional, está sujeito a incertezas e às implicações que eles podem acarretar. A avaliação desses riscos, mesmo que inconsciente, é usada como subsídios para a tomada de decisões, de acordo com a predisposição de cada indivíduo (pessoa ou organização) a aceitá-los ou reduzi-los na expectativa de que o propósito inicial seja alcançado.

Gestão de riscos pode ser definida como a "arquitetura para gerenciar riscos (princípios, estrutura e processo)", enquanto gerenciamento de riscos refere-se à "aplicação dessa arquitetura" [ABNT 2009].

Todas as organizações gerenciam seus riscos, mesmo que não haja uma arquitetura de definida. No entanto, essa abordagem não permite uma visão ampla de todos os elementos, internos e externos, envolvidos no contexto organizacional, nem tampouco fornece recursos que permitam prever e se adiantar às ocorrências indesejáveis. Dessa forma, a instituição simplesmente reage aos eventos não previstos, ocasionando má utilização da força de trabalho e, numa perspectiva mais pessimista, levando a decisões precipitadas que podem causar consequências ainda piores.

Para garantir que os riscos sejam gerenciados "de forma eficaz, eficiente e coerente" é necessário que se tenha uma "estrutura sistemática, transparente e confiável" [ABNT 2009]. A gestão de riscos possibilita conhecer e manipular os fatores relacionados aos riscos, através de um processo lógico e disciplinado. Deste modo, ela se destaca como alternativa para potencializar o alcance os objetivos institucionais, através da identificação de oportunidades e ameaças e aplicação do tratamento adequado a cada caso, no intuito de maximizá-las ou minimizá-las.

Esse processo atua diretamente na melhoria da governança e gestão de TI, pois permite estabelecer uma base confiável para o planejamento e tomada de decisões de forma proativa, aperfeiçoando os controles internos e prevenindo perdas.

No caso das instituições públicas, onde a demanda regulatória é muito intensa, a existência de mecanismos de gestão de riscos definidos ajuda, inclusive, a assegurar o atendimento às normas e requisitos legais, ao detectar pontos vulneráveis a falhas e aplicar o tratamento adequado antes que elas se concretizem.

Dessa forma, considerando a complexidade dos projetos de tecnologia da informação e a rigidez dos contratos celebrados pela Administração Pública, a gestão de riscos atua como importante subsídio para o êxito das aquisições de soluções de TI, uma vez que permite antever possíveis empecilhos do 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.

Ao contrário do que se imagina, terceirizar a concepção de Soluções de TI não elimina a existência de fatores de risco. Nesse caso, a instituição contratante transfere os riscos relativos à execução para a contratada e assume uma série de riscos adicionais, relativos à contratação e à interdependência entre as partes envolvidas.

Em busca, pois, de compreender as abordagens de gestão de riscos utilizadas foram analisados, na presente pesquisa, alguns frameworks que tratam de gestão de riscos, dentre eles, destacaram-se a ABNT NBR ISO 31000, a área de gerenciamento de riscos do PMBOK® e os métodos propostos por modelos específicos para aquisições de TI: CMMI-ACQ e o Guia de Aquisição de Software e Serviços Correlatos do MPS.BR.

4.1. ABNT NBR ISO 31000

A ABNT NBR ISO 31000 (2009) apresenta "princípios e diretrizes genéricas" para a implementação da gestão de riscos. A norma é baseada no padrão internacional, elaborado pela International Organization of Standardization (ISO), e é aplicável a qualquer instituição pública ou privada, independente da área de atuação.

A norma apresenta os princípios que uma organização deve seguir para que tenha uma gestão de riscos eficaz e, a partir deles apresenta um modelo de estrutura para

implantá-la e mantê-la progressivamente. Por fim, a norma propõe um modelo de processo de gestão de riscos.

Destaca-se que, apesar do nível de detalhamento, não é intuito da norma padronizar o processo nem a estrutura de gestão de riscos nas organizações, mas prover o conhecimento necessário para que cada uma delas avalie a estrutura mais adequada para a sua realidade.

4.2. PMBOK®

Frequentemente, as organizações lançam mão da utilização de projetos como "meio de direta ou indiretamente alcançar os objetivos do plano estratégico" [PMI 2013]. Um projeto é uma atividade temporária empreendida para gerar um determinado resultado, como produtos, serviços, etc. A sua conclusão é dada no momento em que os objetivos do projeto são atendidos, ou quando, por algum motivo, as partes interessadas no projeto não considerem mais viável ou oportuno mantê-lo [PMI 2013].

As contratações de tecnologia da informação devem estar alinhadas aos objetivos estratégicos organizacionais, através da aderência às metas propostas no Planejamento Estratégico de TI. Normalmente essas contratações estão atreladas a projetos, por exemplo, o desenvolvimento ou aquisição de um sistema de informação novo ou modificado, o aprimoramento de um sistema existente, a aquisição de equipamentos necessários para atender um determinado propósito.

Portanto, para fins deste trabalho, considera-se que o processo de contratação de Soluções de TI pode ser gerenciado de maneira análoga a um projeto, pois estão intrinsecamente relacionados. Além disso, mesmo nas contratações cujos objetivos não envolvem a criação de resultados evidentes, como, por exemplo, serviços continuados de manutenção, é possível utilizar estratégias de gerencia de projetos para garantir que o escopo do contrato seja plenamente atendido. Isso porque, mesmo tratando-se de atividades operacionais iteradas, cada contratação é única e temporária e envolve uma série de circunstâncias e situações diferentes a cada renovação.

Com intuito de disseminar o conhecimento relativo às boas práticas em gerenciamento de projetos, o Project Management Institute (PMI) concebeu o Project Management Body of Knowledgment (PMBOK®), que atualmente encontra-se na sua quinta edição. O Guia PMBOK® fornece diretrizes para o gerenciamento de projetos, incluindo o ciclo de vida e os processos associados.

Ao todo, o guia apresenta 47 processos de gerenciamento de projeto, aplicáveis a todo ciclo de vida, organizados em 10 (dez) áreas de conhecimento, que correspondem a atividades de campos profissionais distintos. Dado o escopo deste trabalho, analisou-se detidamente apenas os processos relativos à área de Gerenciamento dos Riscos.

Para o PMI (2013), em se tratando de projetos, "risco é um evento ou condição incerta que, se ocorrer, provocará um efeito positivos ou negativo em um ou mais objetivos do projeto" (escopo, cronograma, custo, qualidade, etc.). Os riscos são inerentes a esse cenário, e a análise desse conjunto fornece o risco geral do projeto, fator a se considerado pelos gestores para tomar decisões relativas à viabilidade de continuidade dos trabalhos. No geral, para que a organização alcance os êxitos esperados, ela deve estar comprometida em abordar o gerenciamento de riscos proativamente, evitando-se problemas decorrentes de ameaças não gerenciadas.

Nesse ínterim, o modelo apresenta uma série de processos para gerenciamento de riscos, relacionando-os às práticas de gestão de projetos e apontando as entradas necessárias, os resultados gerados e algumas ferramentas e técnicas para executá-los.

4.3. CMMI-ACQ

O *Capability Maturity Model Integration for Aquisition* (CMMI-ACQ) é um dos modelos de capacidade e maturidade que compõem o *Capability Maturity Model Integration* (CMMI), desenvolvido pelo *Software Enginnering Institute* (SEI).

> O CMMI-ACQ apresenta um guia para aplicação das melhores práticas do CMMI para aquisições de softwares ou bens e serviços correlatos. O modelo é focado nas atividades de iniciação e gestão da aquisição de produtos e serviços de software, com o intuito de que eles atendam as necessidades previstas inicialmente.

O modelo define uma área de processos de Gestão de Riscos, que descreve as atividades a serem executadas no decorrer do projeto para mitigar os impactos negativos que possam afetar o alcance dos objetivos estabelecidos.

Segundo o modelo, a gestão de riscos deve ser contínua durante todo o ciclo de vida da contratação. A ideia é identificar e avaliar os riscos durante o planejamento do projeto e gerenciá-los nas etapas seguintes. A identificação, a princípio, enfatiza apenas os riscos relacionados com o processo de aquisição, mas na medida em que o projeto avança para a fase de seleção do fornecedor, novos riscos são registrados.

Geralmente, após o contrato firmado, a organização contratante se abstém de realizar o gerenciamento dos riscos, delegando essa obrigação à contratada. O grande diferencial da Gestão de Riscos proposta pelo CMMI-ACQ é enfatizar que a contratante deve continuar gerenciando os riscos do projeto, inclusive no que tange à possibilidade da contratada não cumprir com suas obrigações contratuais.

A Gestão de Riscos do CMMI-ACQ compreende as seguintes metas: (i) *Prepare for Risk Management*, (ii) *Identify and Analyse Risks*, (iii) *Mitigate Risks*. Para cada uma delas estão descritas as atividades necessárias para sua consecução, contendo exemplos de artefatos decorrentes, desenvolvidos tanto pela contratante como pela contratada, algumas técnicas e práticas sugeridas para realizá-las.

4.4. MPS-BR – Guia de Aquisição

No âmbito do mercado brasileiro, a Associação para Promoção da Excelência do Software Brasileiro (SOFTEX) criou em 2003 o programa de Melhoria de Processo do Software Brasileiro (MPS.BR) para melhorar a capacidade de desenvolvimento de software nas empresas brasileiras.

> Com base nas normas internacionais, a SOFTEX estabeleceu o Guia de Aquisição do MPS.BR com o objetivo de orientar as organizações que adquirem ou fornecem software ou serviços/produtos correlatos. Nele estão descritas as "atividades e tarefas fundamentais para garantir a qualidade do contrato e respectivos produtos e serviços entregues pelo fornecedor" [SOFTEX 2013].

O guia descreve 4 atividades básicas: (i) Preparação da aquisição; (ii) Seleção do fornecedor; (iii) Monitoração do contrato; (iv) Aceitação pelo cliente. Para cada uma, estão associadas os objetivos, as tarefas previstas e os produtos requeridos e gerados.

Ao contrário dos outros modelos apresentados, o Guia de Aquisição do MPS.BR não apresenta processo específico para gestão de riscos. No entanto, a necessidade de identificar e gerir riscos da contratação é explorada no decorrer das atividades previstas.

A gestão de riscos é abordada desde o início do processo de contratação na tarefa "Desenvolver uma estratégia de aquisição", prevista na "Preparação da aquisição", a qual contempla levantamento geral dos riscos e eventos que podem ocorrer durante o processo e como devem ser tratados, contendo: identificação dos riscos; probabilidade de ocorrência; impacto no projeto; procedimentos de mitigação dos riscos, para amenizar ou eliminar a possibilidade de que eles se concretizem; e plano de contingência, para aliviar o impacto de riscos efetivados.

Durante a "Seleção do fornecedor", na tarefa "Preparar e negociar um contrato" riscos identificados podem ser complementados ou descartados, enquanto novos riscos podem sem adicionados.

A atividade de "Monitoração do contrato" destina-se a acompanhar e garantir o desempenho do contrato firmado com o fornecedor. O constante monitoramento do projeto provê uma base concisa para a tomada de decisões, permitindo aos gestores antever problemas e gerenciá-los, evitando-se prejuízos maiores. Nesse ponto, a gestão de riscos exerce papel fundamental.

Através de avaliações periódicas ao longo da execução, problemas podem ser identificados e ações de mitigação podem ser empreendidas para minimizar riscos. O guia propõe que seja estabelecido um canal de comunicação aberto para troca constante de informações entre as partes, acerca do progresso técnico e dos custos, bem como a identificação de possíveis riscos. O monitoramento perdura até a entrega final do objeto da contratação e a sua aceitação.

O Guia de Aquisição do MPS.BR é bastante sucinto e limita-se a apresentar o que precisa ser feito, sem detalhar como. No entanto, para esta pesquisa, é importante conhecer a abordagem utilizada por trata-se de um modelo adaptado à realidade das organizações brasileiras. No que se refere à gestão de riscos, ele é bastante incipiente, mas essa abordagem também deve ser considerada, a fim de alcançar o equilíbrio entre a complexidade da gestão de riscos e o valor que ela agrega às contratações.

5. Resultados

Todos os modelos analisados reconhecem a relevância dos riscos e apresentam processos específicos que podem ser facilmente integrados aos trâmites legais exigidos, de modo que essas rotinas possam ser incorporadas aos procedimentos existentes nas instituições sem óbice, inclusive no que tange aos papéis desempenhados. Além disso, é importante destacar que os modelos estudados não são exclusivos entre si, mas se complementam, de acordo com o contexto em que são empregados. Observa-se, portanto que todos os objetivos da pesquisa foram plenamente alcançados.

Acredita-se que o presente estudo contribuirá diretamente para prover meios de melhorar a eficácia das aquisições de TI, uma vez que, devido à complexidade desses projetos e o rigor das contratações públicas, a definição de mecanismos sólidos de gestão de risco é fundamental para garantir alcance dos benefícios pretendidos.

Além disso, pretende-se que esses resultados fomentem a realização de novas pesquisas nas áreas de contratação de TI e gestão de riscos na Administração Pública, pois ainda há grande carência de estudos específicos relacionados a essas temáticas.

Cumpre ressaltar que o escopo deste trabalho não pretende exaurir todos os modelos de gestão de riscos que podem ser aplicáveis às contratações públicas de tecnologia da informação, tendo em vista a ampla abrangência do tema. Caso seja preciso adaptar a pesquisa para uso de outros referenciais teóricos, é possível que se

realize o mesmo estudo, seguindo-se os métodos propostos, com adequação das fontes para o objetivo necessário.

Por fim, como trabalhos futuros, pretende-se elaborar um modelo de gestão de riscos específico para as aquisições de TI na APF integrado ao processo existente, de acordo com os modelos apresentados nessa pesquisa, e avaliar a implantação desses mecanismos.

Referências

Associação Brasileira de Normas Técnicas (ABNT) (2009). NBR ISO/IEC 12207. Rio de Janeiro, RJ.

Associação Brasileira de Normas Técnicas (ABNT) (2009b). NBR ISO/IEC 31000. 1ª Edição. Rio de Janeiro, RJ.

Brasil (2012). Tribunal de Contas da União. Acórdão 2.585-38/2012-TCU-Plenário. Relatório de Levantamento. Brasília, DF.

Brasil (2014). Instrução Normativa nº 4 de 11 de setembro de 2014. Diário Oficial da União, Brasília, DF, n. 176, 12 set. 2014, Seção 1, p.96-99.

Brasil (2014b). Tribunal de Contas da União. Acórdão 3117/2014–TCU–Plenário. Relatório De Levantamento. Brasília, DF.

Prodanov, C. C e Freitas, E. C. (2013). Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. Novo Hamburgo, RS: Universidade Feevale, 2ª Edição.