TRIBUNAL DE CONTAS DO ESTADO DO CEARÁ
REVISTA Controle Doutrinas e Artigos
ISSN 1980-086X e-ISSN 2525-3387
www.revistacontrole.tce.ce.gov.br

Percepção dos gestores de Tecnologia da Informação sobre as práticas de gestão de riscos nas aquisições de TI do município de Fortaleza à luz da NBR ISO 31000

Perception of Information Technology managers about the risk management practices in IT acquisitions of the Municipality of Fortaleza in the light of NBR ISO 31000

https://doi.org/10.32586/rcda.v22i1.874

Alexsandro Araújo da Silva[1]
Mariângela Araújo Pinto Bezerra[2]
Jorge Alberto Cavalcanti Alcoforado[3]
Airton Douglas de Andrade Lucas[4]
Alessandra Carvalho de Vasconcelos[5]

RESUMO

A gestão de riscos no setor público constitui instrumento gerencial primário para os gestores, em especial para aumentar a segurança e o desempenho na implementação das políticas públicas. Nesse sentido, este

1 Graduado como tecnólogo em processamento de dados (FCTFOR), MBA em Gestão de Projetos (FGV), MBA em Gestão de Negócios (USP) e Mestrando em Administração e Controladoria pela UFC. Atuou como gerente de governança de TI e atualmente é gerente de desenvolvimento de soluções de tecnologia, ambos na Secretaria Municipal das Finanças de Fortaleza. E-mail: alex.araujo.silva@gmail.com

2 Graduada em Informática pela Universidade de Fortaleza (Unifor), Especialista em Engenharia de Software pela Unifor e Mestranda em Administração e Controladoria pela UFC. Atuou como gerente de soluções na Xerox Corporation, gerente de projetos na Indra. Atualmente é gerente de TIC na Secretaria Municipal de Finanças de Fortaleza. E-mail: mariangelapinto@gmail.com

3 Graduado em Sistemas de Informação pela Universidade Sete de Setembro (UNI7), Especialista em Gestão Pública Municipal pela UECE e Mestrando em Administração e Controladoria pela UFC. Atuou como coordenador de TIC na Secretaria de Planejamento e Gestão do município de Fortaleza. Atualmente é coordenador de TIC na Secretaria Municipal de Finanças de Fortaleza. E-mail: jalcoforado@gmail.com

4 Graduado em Direito pela Unifor, Especialista em Direito Processual Civil, individual e Coletivo pela Unichristus e Mestrando em Administração e Controladoria pela UFC. Atuou como supervisor jurídico da Embracon e como coordenador jurídico da Sepog-PMF e da Segov-PMF, ambas do município de Fortaleza, nesta última foi secretário executivo. Atualmente é procurador assistente na Procuradoria-Geral do Município de Fortaleza. E-mail: douglaslucasadv@gmail.com

5 Graduada em Ciências Econômicas e em Ciências Contábeis pela Unifor, Mestre em Ciências Contábeis pela Fundação Universidade Regional de Blumenau (Furb) e Doutora em Engenharia de Produção pela UFSC. Pesquisadora do CNPq e Professora Associada da Universidade Federal do Ceará no curso de Graduação em Ciências Contábeis e no Programa de Pós-Graduação em Administração e Controladoria acadêmico e profissional. E-mail: alevasconcelos.ufc@gmail.com

artigo tem por objetivo analisar, à luz da NBR ISO 31000:2009, a aderência de boas práticas de gestão de riscos nas aquisições de Tecnologia da Informação (TI) da Prefeitura Municipal de Fortaleza (PMF). A pesquisa descritiva utilizou como procedimentos o *survey*, e quanto à abordagem do problema caracteriza-se como qualitativa. Para tanto, um questionário estruturado no formato de *checklist* foi aplicado junto aos representantes do Grupo Técnico de Tecnologia da Informação e Comunicação (TIC) da PMF, nos meses de maio e junho de 2022. Os resultados apontam que os processos de tratamento de riscos e o registro do processo de gestão de riscos foram os que registraram menos aderência. Conclui-se que, de forma geral, há baixa aderência dos processos relacionados à gestão de riscos nas aquisições de TI pela PMF considerando-se a NBR ISO 31000:2009. Várias reflexões podem ser realizadas a partir dos resultados no sentido de gerar uma evolução do processo de gestão de riscos ligados ao processo de aquisição de TI na PMF. Os processos da norma apresentam-se como norteadores para a própria melhoria.

Palavras-chave: gestão de riscos; NBR ISO 31000:2009; setor público.

ABSTRACT

Risk management in the public sector is a key tool for managers to increase safety and performance in the implementation of public policies. Thus, this paper aims to analyze, through the NBR ISO 31000:2009, the adherence to good risk management practices in the acquisitions of Information Technology (IT) by the Municipality of Fortaleza (PMF). The descriptive research used as procedures the survey and as the approach to the problem is characterized as qualitative. To this end, a structured questionnaire in the form of a checklist was applied to representatives of the PMF's ICT Technical Group, in the months of May and June 2022. The results indicate that the risk treatment and risk management process registration processes were the ones that recorded least adherence. It is concluded that, in general, there is low adherence to the processes related to risk management in IT acquisitions by the PMF, considering NBR ISO

31000:2009. Several reflections can be carried out from the results in order to generate an evolution of the risk management process linked to the PMF's IT acquisition process. The standard`s processes are presented as guides for the improvement itself.

Keywords: risk management; NBR ISO 31000:2009; public sector.

Avaliado pelo sistema double blind review (SEER/OJS – versão 3)

Data de submissão: 23/05/2023
Data de aprovação: 31/07/2023
Data de versão final: 20/09/2023
Data de publicação online: 11/12/2023

1 INTRODUÇÃO

No caminho de uma governança pública em prol da sustentabilidade, segundo afirma Moraes (2020), o gerenciamento de riscos vem ganhando importância na gestão das organizações do setor público. A partir de experiências no manejo de incertezas a que estão sujeitas quaisquer organizações, a gestão de riscos no âmbito público constitui importante instrumento gerencial para os administradores, em especial para aumentar a segurança e o desempenho na implementação das políticas públicas. Ademais, conforme elucida Ávila (2014, p. 180), "o sucesso na implementação do gerenciamento de risco deverá resultar em melhorias na qualidade dos serviços públicos e a eficácia das políticas públicas, também para os municípios brasileiros".

No entanto, Garcez (2019) reforça que a ausência de regras específicas e adequadas que pudessem guiar a inserção da gestão de riscos como prática retardou sua implementação no setor público. Nessa perspectiva, Santos (2017) esclarece que a norma ISO 31000:2009 – *Risk Management – Principles and Guidelines on Implementation* – considera o risco como sendo o efeito da incerteza sobre os objetivos. Esse efeito, no caso, é um desvio em relação ao esperado, podendo ser positivo ou negativo.

Em consonância com parâmetros internacionais, a Associação Brasileira de Normas Técnicas (ABNT, 2009) publicou a NBR ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes, que registra o mesmo conceito.

Segundo Martin, Santos e Dias Filho (2004), a Controladoria tem como algumas de suas funções identificar, mensurar, analisar, avaliar, divulgar e controlar os diversos riscos envolvidos no negócio, bem como seus possíveis efeitos. Nesse contexto, a PMF, por meio da Secretaria de Planejamento e Gestão (Sepog), criou o Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação (Sistic) regulamentado pelo Decreto nº 13.566, de 7 de abril de 2015, e que tem como função gerir o processo decisório no âmbito da TIC.

Através do Sistic, foi definido, por meio da Instrução Normativa Sepog nº 2, de 24 de janeiro de 2019, um novo método de aquisição de Tecnologia da Informação e comunicação (TIC) na PMF (FORTALEZA, 2019), quando se definiu que toda aquisição fosse submetida a uma análise prévia. Com essa ação, a PMF projeta uma diminuição da probabilidade de ocorrência de problemas, seja de conformidade, *compliance* ou simplesmente fora de diretrizes predefinidas.

Como afirmam Walraven *et al*. (2023, p. 13), "a gestão de risco possibilita às organizações identificarem e gerenciarem riscos e oportunidades, contribuindo para mitigar incertezas e aumentar a probabilidade de alcançar os seus objetivos". Nessa ótica, em decorrência da disciplina de gestão de riscos, os órgãos públicos passaram a adotar, mesmo que instintivamente, procedimentos precisos e rigorosos de controle dos riscos inerentes às suas atividades. Nesse ambiente de insegurança, tornou-se inevitável a demanda por normas, metodologias e ferramentas capazes de lidar com os riscos.

Diante da importância da temática para as organizações públicas, o estudo de Soares Netto (2013), aplicado no âmbito federal, fez uso da NBR ISO 31000:2009 nas contratações de TI. O autor propôs uma ferramenta focada especificamente na identificação de riscos, e serviu como fator motivador para a elaboração do presente artigo. Assim, esta pesquisa empírica,

aplicada especificamente no âmbito municipal, objetiva preencher a lacuna caracterizada pela falta de uma análise das contratações de TIC, perpassando, com um olhar mais amplo, todos os processos da ISO 31000:2009, não direcionados exclusivamente para a identificação de riscos.

Segundo Bitencourt (2019), a gestão de riscos constitui uma das principais preocupações da sustentabilidade no contexto das organizações, tornando-se de suma importância a sua compreensão e a de seus componentes. O cenário de mudanças, a elevada competitividade e a incerteza que cerca o ambiente organizacional remetem a grandes desafios e a muitos riscos. Nesse contexto, a governança corporativa, o *compliance* e a gestão de riscos são ferramentas de gestão obrigatórias (TRIVELATO; MENDES; DIAS, 2018).

Do exposto, o presente estudo se insere no campo da implementação de políticas públicas de apoio à melhoria da gestão, tendo como foco a análise das boas práticas de governança, sob o olhar da gestão de riscos nas aquisições de Tecnologia da Informação (TI) pela Prefeitura Municipal de Fortaleza (PMF). Assim, com base na NBR ISO 31000:2009, este artigo toma por diretriz a seguinte questão de pesquisa: qual o nível de aderência de boas práticas de gestão de riscos nas aquisições de Tecnologia da Informação na Prefeitura Municipal de Fortaleza?

Logo, o presente artigo tem como objetivo geral analisar, à luz da NBR ISO 31000:2009, a aderência de boas práticas de gestão de riscos nas aquisições de TI pela PMF.

Esta pesquisa tem sua importância evidenciada, pois, apesar de existirem alguns estudos prévios sobre a gestão de riscos nas aquisições de TIC, como, por exemplo, os de Silva, Oliveira e Canedo (2016) e Nobre (2017), não foi percebida uma análise estruturada e comparativa com a ISO 31000:2009 por meio de um instrumento, como é proposto neste artigo. A maioria dos estudos empíricos concentra-se no planejamento das aquisições. Segundo Soares Netto (2013), para suprir essa lacuna, faz-se necessário um apoio metodológico ou procedimental. Dessa forma,

é possível a utilização da gestão de riscos baseada na norma NBR ISO 31000:2009, cuja utilização pode ser destinada às contratações de TICs, haja vista que o gerenciamento dos riscos tem sido utilizado por organizações de diversos segmentos devido a sua aplicabilidade multidisciplinar.

Outra contribuição importante desta pesquisa reside na sua aplicação no âmbito municipal, aprofundando a discussão sobre a responsabilidade fiscal no âmbito público, ao mostrar evidências da relação entre os riscos e o processo decisório. Ao descrever a situação atual da PMF, no que tange à aderência com ferramentas de boas práticas de gestão de riscos, a pesquisa contribui para a idealização de um modelo comparativo que, com as devidas adaptações, poderá ser replicado a outras realidades em outros entes públicos.

A análise resultante da aplicação do instrumento de avaliação na PMF poderá possibilitar a associação de riscos e decisões e o entendimento das pressões que sofrem os gestores públicos municipais, mais especificamente da área de TIC, nas questões norteadoras, éticas e ambientais em seus modelos de negócio.

Ao se desenvolver a pesquisa, a intenção era de que, à luz da NBR ISO 31000:2009, seja possível identificar o nível da aderência das decisões tomadas sobre aquisições de TI na unidade de análise estudada. Essa aplicação deverá servir de referência para outros gestores, no apoio ao processo decisório no que tange as aquisições de TI, com a possibilidade de se expandir para outros aspectos da governança que envolvam riscos. Vale ressaltar que, no primeiro momento, o instrumento de avaliação adotado nesta pesquisa poderá ser replicado na própria PMF e em outros entes públicos.

2 REFERENCIAL TEÓRICO

Nesse tópico é apresentado o embasamento teórico da pesquisa. Para tanto, são abordadas as temáticas gestão de riscos e a NBR ISO 31000:2009, e gestão de riscos e o processo de compras públicas. Em seguida, são resgatados estudos prévios sobre a temática aqui analisada.

2.1 Gestão de riscos e a NBR ISO 31000:2009

Denomina-se gestão de riscos, o conjunto de atividades coordenadas para se identificar, analisar, avaliar, tratar e monitorar riscos. Dependendo do porte e da complexidade das operações, as organizações adotam abordagens informais, bem como, estruturadas e sistematizadas, para gestão de riscos visando alcançar objetivos. A gestão de riscos também é definida como o processo que trata da criação, distribuição e preservação de valor para as organizações (VIEIRA; BARRETO, 2019).

No ambiente empresarial, a gestão de riscos vem despertando muita atenção; contudo, esse assunto não é novo. Sob o olhar de controles internos, a auditoria interna contribui para melhorar a gestão de riscos (PENHA; PARISI, 2005).

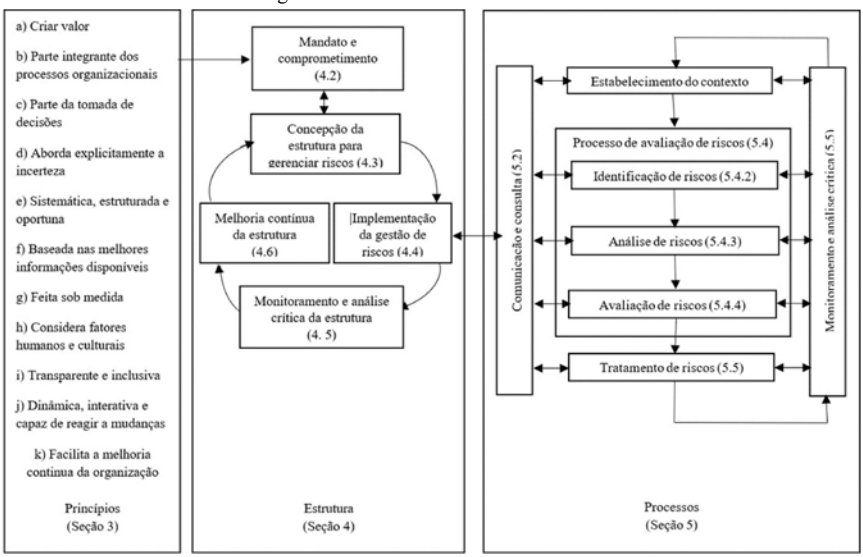
Segundo Fernandes, Kroenke e Söthe (2009), o controle focado na gestão de riscos operacionais revela-se fundamental para prever, classificar e mitigar os riscos presentes em todas as decisões. Isso pode reduzir a probabilidade de eventos inesperados e outras perdas resultantes de riscos não calculados. É importante que esse controle seja realizado por uma equipe especializada, ou seja, que não desempenhe outra atividade além do controle de riscos operacionais, pois se trata de um trabalho complexo e de grande responsabilidade (FERNANDES *et al*., 2009).

A gestão de riscos tem a responsabilidade de implantar um processo de administração eficiente e continuado nas organizações, visando à melhoria contínua por meio da redução de prejuízos e aumento dos benefícios. Há, no entanto, a necessidade de uma padronização de conceitos, pressupostos, regulamentações e *frameworks*, que auxilie as organizações a gerir seus riscos de forma eficiente, eficaz e coerente. Nesse sentido, a norma ISO 31000:2009 foi desenvolvida originalmente pela *International Organization for Standardization* (ISO), com a participação de especialistas de mais de 30 países. Dessa forma, a NBR ISO 31000:2009 pode ser

aplicada a qualquer tipo de risco e em qualquer segmento organizacional (SANTOS, 2021).

Gerenciar riscos faz parte da governança e liderança, sendo fundamental para aperfeiçoar a maneira como a organização é gerenciada em todos os níveis, contribuindo para a melhoria dos sistemas de gestão. Gerenciar riscos faz parte do conjunto de atividades associadas com uma organização, e inclui a interação com as partes interessadas, devendo-se considerar os contextos externo e interno, incluindo o comportamento humano e os fatores culturais (ABNT, 2009). Em suma, o gerenciamento de riscos baseia-se nos princípios, estrutura e processos delineados descritos na Figura 1.

Figura 1 – Estrutura da ISO 31000:2009



Fonte: adaptada da ABNT (2009).

A Figura 1 demonstra a estrutura da ISO 31000:2009, que está dividida em três partes: os princípios, que sugerem uma gestão de riscos eficaz, caso estes sejam seguidos; a estrutura, que através de fundamentos e arranjos, propõe eficácia se esta existir em toda a organização; e, os

processos de gestão de riscos, que pressupõem a aplicação sistemática das políticas, dos procedimentos e das práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos (ABNT, 2009).

Convém que o processo de gestão de riscos seja parte integrante da gestão e do processo decisório, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas e de projetos, sendo possíveis muitas aplicações no processo de gestão de riscos personalizadas para alcançar os objetivos e para se adequar aos contextos externo e interno nos quais são realizadas. Nessa perspectiva, Junqueira (2021) reforça que, conforme preconiza a ABNT NBR ISO 31000:2009, é importante que se levem em conta a natureza dinâmica e variável do comportamento humano e a cultura. Portanto, a relação entre os componentes do processo de gestão de riscos, a comunicação e consulta e o monitoramento e análise crítica ocorre em todas as etapas.

Do exposto, de forma genérica, Klein Junior (2020, p. 1) menciona que "diferentes governos têm adotado a gestão de riscos como parte de um novo padrão de excelência para o controle interno" e que "uma nova lógica de *accountability*, por meio da qual órgãos de controle devem redefinir os limites da ação e responsabilidade pública" deve ser implementada pelos entes públicos.

2.2 Gestão de riscos e o processo de compras públicas

Com enfoque mais específico, Parreira (2018) alerta que as aquisições envolvendo a Tecnologia da Informação e Comunicação (TIC) geralmente são complexas e burocráticas, exigindo profundo conhecimento técnico no assunto, além de competência para se planejar e gerir adequadamente a contratação, de acordo com a legislação vigente. No mesmo

sentido, Pires, Cavalcante e Correa (2016) afirmam que as incertezas geradas por problemas financeiros, recursos humanos e recursos tecnológicos trazem diversos riscos e inseguranças para os gestores, e em muitos casos acarretam interrupções no processo licitatório e atrasos em entregas.

Importante salientar que, de acordo com o documento Referencial básico de gestão de riscos, do Tribunal de Contas da União (2018a), a falta de procedimentos sistemáticos faz com que os riscos envolvidos durante a contratação de TIC não sejam efetivamente gerenciados, podendo acarretar o insucesso no alcance das metas e objetivos organizacionais.

Outrossim, conforme o TCU (2018b) elucida, 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.

Particularmente em relação às compras públicas, Munnukka e Järvi (2015) e Santos, Martins e Freitas (2023) destacam que os riscos estão presentes, em diferentes graus, em todos os processos de compras e, por isso, precisam ser gerenciados.

Nishiyama *et al*. (2017) e Mourão e Marinho (2022) enfatizam que, nas últimas quatro décadas, as pressões por uma gestão mais transparente e eficiente têm desafiado os pesquisadores a propor novos métodos para apoiar a gestão de compras públicas.

Segundo Terra (2018), isso se dá porque uma das áreas mais sensíveis e importantes dentro da administração pública constitui-se nas compras públicas, contudo, estas ainda carecem de aperfeiçoamentos. Tais ajustes, como em outros países, não caracterizam um processo simples, pois envolve muitas mudanças e produz impactos, quer sejam culturais, estruturais, governamentais, administrativos e legislativos (TERRA, 2018).

Dessa forma, tratar riscos em aquisições de bens públicos são atividades de controle interno que compreendem processos (identificar, entender, avaliar e tratar os eventos que possam ter a consequência de impactar negativamente os objetivos do procedimento) e atitudes (evitar, aceitar, trans-

ferir e mitigar). Para tanto, pode-se fazer uso de algumas técnicas, ações e ferramentas para tal, a saber: capacitação, normatização, manuais, roteiros, segregação de funções, tecnologias, *checklists* etc. (SOARES, 2019).

Ademais, Cardoso e Alves (2020) ponderam que aquisições que envolvem ativos e serviços de TI, na administração pública, apesar do aparato legal que suporta o processo de aquisição, costumam ser bastante complexas e burocráticas, o que exige dos profissionais envolvidos bom conhecimento técnico e competências para gerir tais aquisições.

Do exposto, instrumentos capazes de assessorar gestores de TIC no controle dos riscos nos processos de aquisição passam a ser fundamentais. Segundo Cardoso (2019), além da complexidade inerente aos processos de TIC, a rotatividade dos atores envolvidos e as particularidades de cada equipe de planejamento da contratação, torna-se essencial definir procedimentos práticos e sistematizados que possam ser utilizados para identificar, analisar, avaliar, tratar, monitorar, controlar, documentar e informar riscos envolvendo as aquisições de TIC. Diante da relevância da temática, foram desenvolvidos alguns estudos empíricos sobre o assunto, sendo alguns deles descritos brevemente a seguir.

2.3 Estudos empíricos anteriores

O Quadro 1 apresenta de forma sucinta alguns estudos correlatos, nacionais e estrangeiros, que, assim como a presente pesquisa, e amparados na NBR ISO 31000, investigaram a gestão de riscos e a gestão de aquisições de TIC em diferentes contextos organizacionais.

Quadro 1 – Estudos empíricos anteriores

Autoria	Objetivo	Principais resultados
Keller e Köhler (2021)	Conciliar conhecimentos teóricos de diferentes disciplinas e vinculá-los à experiência prática, dando uma estrutura clara, com atividades, técnicas e resultados direcionados por etapa do processo que estão prontos para uso pelos profissionais.	Propor um quadro abrangente para o risco de avaliação de novas tecnologias em oferta da gestão de cadeia. Para tanto, foram usadas metodologias já existentes, especialmente seis metodologias de avaliação de riscos, bem como, quatro métodos de avaliação de riscos de segurança de TI.
Cardoso e Alves (2020)	Apresentar as etapas para a construção de uma metodologia sistematizada para gestão de riscos em aquisições de TIC no âmbito das instituições públicas brasileiras.	Constatou-se que para se obter a melhoria contínua do processo, a maximização da transparência dos atos administrativos e o aprendizado colaborativo, pode-se utilizar o compartilhamento de lições aprendidas por meio de um inventário de riscos, um mapa de gerenciamento de riscos e um repositório digital de informações.
Nobre (2017)	Propor a elaboração de uma metodologia para gestão de riscos dos processos de aquisição de TI da Fundação Nacional de Saúde (FUNASA).	Os resultados demonstram que a metodologia proposta apresenta viabilidade de utilização nos órgãos públicos federais como meio de auxiliar a internalização de procedimentos previstos na legislação e o aprofundamento do tema gestão de riscos nas contratações de TI na Administração Pública Federal.
Oliveira *et al*. (2017)	Propor um caminho para empresas desenvolverem seus procedimentos e para gerenciarem os riscos na cadeia de suprimentos, com base na ISO 31000:2009, Seção 5.4 (Processo de avaliação de risco).	Os resultados indicam que a ISO 31000:2009 pode ser utilizada de forma benéfica como um método padronizado para executar o gerenciamento de riscos da cadeia de suprimentos, desde que as ferramentas e técnicas sejam selecionadas conforme as necessidades da empresa e as características do negócio.
Soares Netto (2013)	Desenvolver um artefato para a identificação de riscos no processo de contratação de TI na administração pública federal, à luz da norma NBR ISO 31000.	Constatou-se que, com o uso do artefato, os gestores podem encontrar vulnerabilidades que antes não eram observadas, o que possibilitará uma melhoria na definição dos níveis de serviço e na gestão contratual, por meio de uma construção mais eficaz do termo de referência. Os resultados demonstram que o artefato servirá como uma fonte consolidada de informações para identificação de riscos nas contratações de TI na administração pública federal.

Quadro 1 – Estudos empíricos anteriores (continuação)

Autoria	Objetivo	Principais resultados
Scannell, Curkovic e Wagner (2013)	Determinar se a NBR ISO 31000 fornece a estrutura para se chegar a um consenso sobre o escopo e a definição da Gestão de Riscos na Cadeia de Suprimentos (SCRM), e examinar se a NBR ISO 31000 fornece a base para o planejamento e execução da SCRM.	Verificou-se que as empresas reconhecem a importância da SCRM, mas faltam a integração e as habilidades.

Fonte: pesquisa própria (2023).

As informações evidenciadas no Quadro 1, que descrevem os objetivos e os principais achados dos estudos correlatos identificados na revisão de literatura, ressaltam a relevância da presente pesquisa, (i) por considerar todos os processos da NBR ISO 31000:2009, para a avaliação de aderência por meio de um instrumento de verificação e (ii) por viabilizar sua utilização no âmbito de uma prefeitura.

Cabe destacar que a revisão de literatura possibilitou a identificação de estudos importantes envolvendo, direta ou indiretamente, as temáticas gestão de riscos e compras públicas de TIC, entretanto, eles adotaram abordagens diversas do presente estudo. Em suma, Keller e Köhler (2021) realizaram a proposição de um quadro abrangente para avaliação de riscos, enquanto Cardoso e Alves (2020) fizeram uma proposição de uma metodologia para gestão de riscos em aquisições. Nobre (2017), por sua vez, propôs uma metodologia voltada para uso em órgãos públicos federais com foco em gestão de riscos em contratações. Na mesma perspectiva, Oliveira *et al*. (2017) fizeram uso específico da ISO 31000 vislumbrando especificamente o processo de avaliação. Soares Netto (2013) propôs um artefato para identificação de riscos em contratações de TI, baseado na ISO 31000. Scannell, Curkovic e Wagner (2013) verificaram se a ISO 31000 é adequada para o planejamento e execução da gestão de riscos voltados para a cadeia de suprimentos. Já o estudo proposto neste artigo, visa verificar a percepção dos gestores de TI sobre o nível de ade-

rência das práticas de gestão de riscos no processo de aquisições de TIC no município de Fortaleza à luz da NBR ISO 31000:2009, perpassando por todos os processos da norma.

3 METODOLOGIA

Neste tópico, serão apresentados a tipologia da pesquisa, os procedimentos de coleta de dados e, por fim, os procedimentos de análise de dados adotados para consecução do objetivo proposto.

3.1 Tipologia da pesquisa

Esta pesquisa descritiva foi realizada com o intuito de se identificar o nível de aderência da gestão de riscos nas aquisições de TI na PMF, por meio da obtenção de dados primários, a partir da aplicação de um questionário, observando-se as orientações normativas da NBR ISO 31000:2009. Quanto à abordagem do problema, a pesquisa é qualitativa. Quanto aos procedimentos, a pesquisa classifica-se como *survey*, sendo a coleta dos dados feita através de questionário. Conforme Freitas *et al*. (2000, p. 105), a pesquisa *survey* pode ser delineada como "a obtenção de dados ou informações sobre características, ações ou opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo, por meio de um instrumento de pesquisa, normalmente, um questionário".

Para a pesquisa, utilizou-se uma amostragem não probabilística do tipo amostragem por conveniência, ou seja, a escolha de participantes em função de sua disponibilidade. O questionário foi aplicado junto aos oito representantes do Grupo Técnico de TIC (GTTIC) da PMF no período de realização da pesquisa (20 de maio a 3 de junho de 2022). O critério de seleção dos sujeitos da pesquisa levou em consideração a realização da atuação técnica e operacional por parte dos oito representantes selecionados. Estes membros têm um contato mais próximo com o processo, sendo os demais membros do GTTIC, possuidores de um papel de alto nível de decisão, que

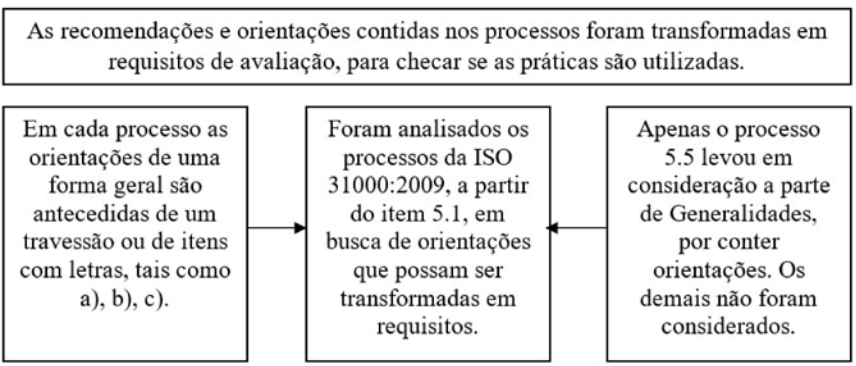
dependem do respaldo técnico do grupo selecionado. Assim, os participantes da pesquisa reúnem os técnicos do GTTIC da PMF (em junho/2022 – período de coleta de dados) que atuavam diretamente no processo de gestão de riscos nas aquisições de TI do município de Fortaleza.

Nesse sentido, o resultado obtido por meio do questionário tem o intuito de descrever a situação atual, em termos de aderência com ferramentas de boas práticas de gestão de riscos, e contribui para a idealização de um modelo comparativo, o qual poderá, após as devidas adaptações, ser replicado a outras realidades em outros entes da gestão pública.

3.2 Procedimentos de coleta de dados

A Figura 2 exibe uma visão geral o método utilizado para a elaboração do instrumento de coleta de dados em formato de *checklist*.

Figura 2 – Método utilizado para a elaboração do instrumento em formato de checklist



Fonte: pesquisa própria (2023).

Conforme mostra a Figura 2, na ISO 31000:2009, foi considerada a parte dos processos da norma, a partir do processo 5. Geralmente no início de cada um dos processos existe um item "Generalidades", que faz uma contextualização ou definição inicial. Somente o item 5.5, apresentou nesta parte de generalidades, opções que foram consideradas como orientações e que poderiam ser modificadas em formato de requisito para geração da avaliação.

Em cada um dos processos, os itens que foram elencados para geração dos requisitos vinham precedidos de um travessão, de itens do alfabeto a), b), c) e em último caso em formato de texto livre. Coube aos pesquisadores esta ponderação, de uma forma estruturada, como citado anteriormente, e evitando uma abordagem mais subjetiva. O Quadro 2 apresenta de forma mais prática e clara, as orientações e sua forma transformada para requisito de avaliação na pesquisa.

Quadro 2 – Transformação das orientações em requisitos do *checklist*

Recomendações	Requisitos para o checklist
Auxiliar a estabelecer o contexto apropriadamente.	O contexto é avaliado e estabelecido apropriadamente?
Assegurar que os interesses das partes interessadas sejam compreendidos e considerados.	Os interesses das partes interessadas são compreendidos e considerados?
Auxiliar a assegurar que os riscos sejam identificados adequadamente.	Os riscos são identificados adequadamente?
Reunir diferentes áreas de especialização em conjunto para análise dos riscos.	As diferentes áreas de especialização são reunidas em conjunto para análise dos riscos?
Assegurar que diferentes pontos de vista sejam devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos.	Os diferentes pontos de vista são devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos?
Garantir o aval e o apoio para um plano de tratamento.	É dado o aval e o apoio para um plano de tratamento de riscos?
Aprimorar a gestão de mudanças durante o processo de gestão de riscos.	A gestão de mudanças é aprimorada durante o processo de gestão de riscos?
Desenvolver um plano apropriado para comunicação e consulta interna e externa.	São desenvolvidos planos apropriados para comunicação e consulta interna e externa?

Fonte: pesquisa própria (2023).

O Quadro 2 apresenta o processo de geração dos requisitos de avaliação a partir das orientações contidas no processo 5.2 – Comunicação e Consulta. Alguns processos possuíam subitens, que foram detalhados da mesma forma.

3.3 Procedimentos de análise de dados

A análise dos dados obtidos com a aplicação do questionário junto aos técnicos do GTTIC da PMF foi realizada com base nos parâmetros descritos

nas Tabelas 1 e 2, fazendo-se uso de análise descritiva e utilizando o software Microsoft Excel para o tratamento dos dados, bem como, a elaboração dos gráficos relacionados aos processos em particular e uma visão geral.

A Tabela 1 apresenta uma visão sintética dos processos e do número de requisitos que foram elencados para cada processo.

Tabela 1 – Estruturação da pesquisa segundo os processos da NBR ISO 31000:2009

Processos	Número de requisitos	Escore máximo
5.2 Comunicação e consulta	8	24
5.3 Estabelecimento do contexto	28	85
5.4 Avaliação de riscos	21	63
5.5 Tratamento de riscos	18	54
5.6 Monitoramento e análise crítica	5	15
5.7 Registro do processo de gestão de riscos	7	21
Total	**87**	**262**

Fonte: pesquisa própria (2023).

Destaque-se que os processos da NBR ISO 31000:2009 utilizados como base de avaliação da aderência na pesquisa são divididos em subprocessos. Assim, o processo 5.3 – Estabelecimento do contexto contempla os subprocessos: 5.3.1 – Estabelecimento do contexto externo; 5.3.2 – Estabelecimento do contexto interno; 5.3.3 – Estabelecimento do contexto do processo de gestão de riscos; e 5.3.4 – Definição dos critérios de riscos. O processo 5.4 – Avaliação de riscos é dividido em: 5.4.1 – Identificação de riscos; 5.4.2 – Análise de riscos; e 5.4.3 – Avaliação de riscos. O processo 5.5 – Tratamento riscos também é dividido em três subprocessos: 5.5.1 – Generalidade; 5.5.2 – Seleção das opções de tratamento de riscos; e 5.5.3 – Preparando e implementando planos para tratamento de riscos. Para efeito de avaliação dos requisitos da unidade de análise da pesquisa, os requisitos de cada subprocesso, quando existentes, foram considerados.

Nesse ponto, cabe informar que como o questionário em formato de *checklist* aplicado junto aos oito técnicos do GTTIC da PMF foi elaborado

considerando, especificamente, a NBR ISO 31000:2009, não foi realizada nenhuma avaliação estatística acerca da consistência do instrumento, tendo em vista a qualidade técnica da equipe respondente.

Conforme pode ser constatado pelo escore máximo atribuído na Tabela 1, foi utilizada uma escala Likert ímpar de três pontos, para avaliação de aderência para cada processo da NBR ISO 31000:2009 no questionário, sendo adotados os seguintes parâmetros de avaliação: Aderente (3), Parcialmente Aderente (2) e Não Aderente (1). Foi utilizado também o parâmetro Não se Aplica, com valor nulo (0), para sinalizar a não utilização do processo ou subprocesso. A atribuição do escore máximo consignado na Tabela 1 levou em conta a completude de todos os requisitos de um processo, multiplicando-se pelo valor máximo de aderência (3). A utilização de uma escala de três pontos não invalida a original abordagem da escala Likert de cinco pontos. A abordagem ímpar de três pontos com uma graduação maior, uma intermediária e uma opção de graduação mínima é uma boa prática (SILVA JÚNIOR; COSTA, 2014).

Para a avaliação do nível de aderência das práticas de gestão de riscos nas aquisições de TI pela PMF à luz da NBR ISO 31000:2009, foi utilizada a análise dos quartis (Tabela 2).

Tabela 2 – Análise do nível de aderência baseado em quartis

Quartil	Valor inicial	Valor final	Aderência máxima (%)	Nível de aderência
Q1	0,00	65,25	25	Baixo
Q2	65,26	130,50	50	Médio
Q3	130,60	195,80	75	Aderente
Q4	195,90	262,00	100	Forte

Fonte: pesquisa própria (2023).

Conforme evidenciado na Tabela 2, o nível máximo de aderência corresponde a 262 pontos, considerando-se a utilização de todos os critérios de todos os processos.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

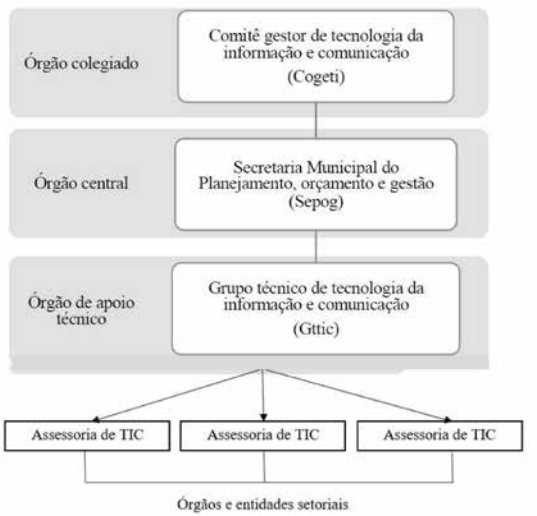
Neste tópico serão expostos os resultados da pesquisa. Para tanto, serão abordadas as temáticas gestão de riscos e a NBR ISO 31000:2009, e a gestão de riscos e o processo de compras públicas. Em seguida, são resgatados estudos prévios sobre a temática aqui analisada.

4.1 Breve descrição do Sistic da Prefeitura Municipal de Fortaleza

Antes de se descrever os resultados da avaliação do nível de aderência das práticas de gestão de riscos nas aquisições de TI pela PMF, cabe apresentar brevemente a estrutura do Sistic da PMF.

Criado por meio do Decreto nº 13.566/2015, o Sistic desempenha as atividades de planejamento, governança, coordenação, organização, aquisição, operação, controle e supervisão dos recursos de TIC dos órgãos e entidades da PMF, com a estrutura organizacional mostrada na Figura 3.

Figura 3 – Estrutura do Sistic



Fonte: pesquisa própria (2023).

Na Figura 3, é possível observar que o Grupo Técnico de TIC (GTTIC), gestores participantes desta investigação, reúne um órgão de apoio técnico que compõe a estrutura do Sistic apresentada na Figura 4, que objetiva viabilizar a tomada de decisões estratégicas no âmbito da PMF, no tocante aos ativos e soluções de TIC.

Figura 4 – Composição do Sistic da PMF

Comitê Gestor de TIC (Cogestic)	Grupo Técnico de TIC (GTTIC)
• Secretários adjuntos ou Secretários executivos • Sepog • Segov • Sefin • CGM • Iplanfor • Citinova	• Coordenador da Cogect • Representante da Sepog • Representante da Sefin • Representante da CGM • Representante do Iplanfor • Representante da Citinova • Representante da SME • Representante da SMS

Fonte: pesquisa própria (2023).
Legenda: Secretaria Municipal do Planejamento, Orçamento e Gestão (Sepog), Secretaria Municipal de Governo (Segov), Secretaria Municipal das Finanças (Sefin), Controladoria e Ouvidoria Geral do Município (CGM), Instituto de Planejamento de Fortaleza (Iplanfor), Fundação de Ciência, Tecnologia e Inovação de Fortaleza (Citinova), Coordenadoria de Gestão Corporativa da Tecnologia da Informação e Comunicação (Cogect), Secretaria Municipal da Educação (SME) e Secretaria Municipal da Saúde (SMS).

A Figura 4 apresenta os componentes do Sistic, que é formado pelo Comitê Gestor de TIC, por sua vez composto pelos secretários e secretários-adjuntos ou secretários-executivos (ou gestores correspondentes) da Sepog, da Segov, da Sefin, da CGM, do Iplanfor, da Citinova e pelo GTTIC (foco deste estudo), composto pelo gestor da Cogect, pelos secretários e secretários-adjuntos ou secretários-executivos (ou gestores correspondentes) da Sepog, da Sefin, da CGM, do Iplanfor, da Citinova, da SME e da SMS.

Fazendo uma análise baseada nos estudos prévios e nos resultados obtidos pela presente pesquisa, foi possível verificar que os estudos não fazem uma análise considerando todos os processos da Norma ISO

31000:2009, buscando uma aderência a todas as recomendações nela contidas. Os estudos que deram importância aos processos específicos da norma foram desenvolvidos por Soares Netto (2013), que deu um foco ao processo de identificação de riscos (5.4.2) e por Oliveira *et al*. (2017), que abordaram especificamente o processo 5.4 – Avaliação dos riscos e seus subprocessos.

4.2 Nível de aderência das práticas de gestão de riscos nas aquisições de TI pela PMF

Após essa breve descrição da estrutura e da composição do Sistic, a seguir são apresentados os resultados da avaliação da aderência das práticas de gestão de riscos nas aquisições de TI tendo como parâmetro os processos da norma ABNT NBR 31000:2009.

Os resultados da pesquisa quanto à análise do nível de aderência das práticas de gestão de riscos nas aquisições de TI pela PMF correspondem às respostas dadas ao questionário por sete dos oito integrantes do GTTIC, no período de 20/5/2022 a 3/6/2022.

Para a análise do nível de aderência, foram considerados os seis processos evidenciados na Tabela 1 (5.2 a 5.7), com seus respectivos subprocessos. O nível máximo de aderência corresponde a 262 pontos, correspondente à utilização de todos os critérios de todos os processos da NBR ISO 31000:2009, sendo a ponderação feita por meio dos quartis (Tabela 2).

De acordo com o exposto, para cada processo e respectivos subprocessos foi feita a identificação dos níveis de aderência (1 – Não Aderente, 2 – Parcialmente Aderente e 3 – Aderente) das práticas de gestão de riscos nas aquisições de TI pela PMF à luz da NBR ISO 31000:2009, conforme a escala proposta. Um exemplo da análise realizada pode ser visto na Tabela 3 que elucida os resultados do processo 5.2 – Comunicação e consulta.

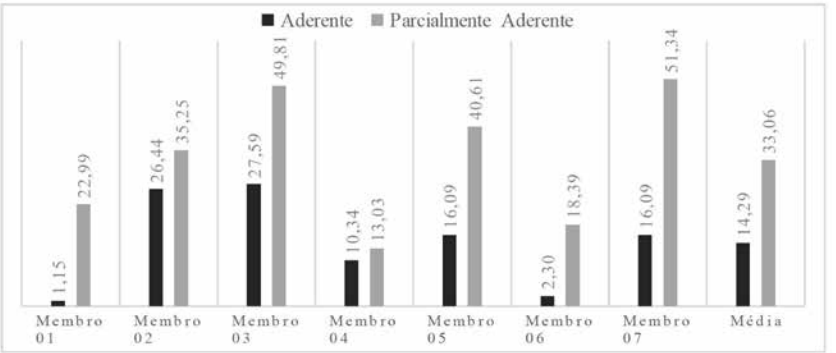
Tabela 3 – Análise do nível de aderência baseado em quartis

Processo 5.2 – Comunicação e consulta		**Nível de aderência**		
Objetivo	Requisito	Aderente	Parcialmente Aderente	Não Aderente
Durante todas as etapas ou atividades do processo de gestão de riscos, deve haver uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas. Avalie as questões alusivas ao processo 5.2 – Comunicação e consulta relacionadas aos riscos.	1. O contexto é avaliado e estabelecido apropriadamente?	3		
	2. Os interesses das partes interessadas são compreendidos e considerados?	3		
	3. Os riscos são identificados adequadamente?		2	
	4. As diferentes áreas de especialização são reunidas para análise conjunta dos riscos?	3		
	5. Os diferentes pontos de vista são devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos?	3		
	6. São dados o aval e o apoio necessários para um plano de tratamento de riscos?		2	
	7. A gestão de mudanças é aprimorada durante o processo de gestão de riscos?		2	
	8. São desenvolvidos planos apropriados para comunicação e consulta internas e externas?		2	
Nível de aderência do processo 5.2 identificado = 20 (ou 83,3%)		**12**	**8**	
Nível de máximo de aderência do processo 5.2 = 24 (ou 100,0%)		**24**		

Fonte: pesquisa própria (2023).

O resultado consolidado das respostas dos participantes do GTTIC quanto à aderência dos seis processos relacionados às práticas de gestão de riscos nas aquisições de TI na PMF (5.2 a 5.7) está apresentado no Gráfico 1.

Gráfico 1 – Nível geral de aderência dos processos de gestão de riscos nas aquisições de TI pela PMF – 31000:2009



Fonte: pesquisa própria (2023).

No Gráfico 1, verifica-se que, de acordo com os membros do GT-TIC, a aderência de todos os processos assinala uma média correspondente a 14,29. Em linhas gerais, as médias de aderência total e de aderência parcial concentram-se abaixo do mínimo esperando no primeiro quartil (65,25), assim, observa-se uma baixa aderência aos processos de gestão de riscos nas aquisições de TI pela PMF em relação à NBR ISO 31000:2009. Destaque-se, entretanto, que nenhum membro considerou não aderentes os processos analisados.

Esse resultado reflete o baixo nível de aderência das práticas de gestão de riscos nas aquisições de TI pelo município de Fortaleza e corrobora a afirmação de Terra (2018) que aponta que apesar de as compras públicas constituírem-se uma das áreas mais sensíveis e importantes da administração pública, estas ainda carecem de aperfeiçoamentos.

Levando-se em consideração a avaliação geral dos resultados (Gráfico 1) e os objetivos de cada processo da ISO 31000:2009, é possível compreender que devem haver evoluções no sentido de:

5.2 – Comunicação e consulta: a comunicação e a consulta às partes interessadas internas e externas, devem acontecer ao longo de todas as fases do processo de gestão de riscos;

5.3 – Estabelecimento do contexto: a organização deve articular seus objetivos, definindo os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecer o escopo e os critérios de risco para o restante do processo;

5.4 – Avaliação de riscos: a organização deve considerar as três vertentes: 1 - identificação, que busca encontrar as fontes de risco, as áreas de impacto, eventos, causas e consequências; 2 - Análise, que trata de desenvolver a compreensão dos riscos, suas fontes, as consequências, quer sejam elas positivas ou negativas e a probabilidade da ocorrência; 3 – Avaliação, com base nos resultados da análise, gerar uma priorização sobre quais riscos merecerão uma resposta;

5.5 – Tratamento dos riscos: a organização deverá selecionar uma ou mais opções para modificar os riscos e a implementação destas;

5.6 – Monitoramento e análise dos riscos: a organização deverá planejar o monitoramento e análise de seus riscos de forma que sejam feitos periodicamente;

5.7 – Registro do processo de gestão de riscos: deve haver por parte da organização, uma preocupação com o registro e rastreamento, em relação a todo o processo de gestão de riscos, permitindo uma evolução continua.

Realizando uma análise analítica dos resultados, a Figura 5 permite uma visão detalhada de cada membro, por cada processo e seus valores de avaliação. A Figura 5 indica valores zerados (que não foram pontuados nos processos pelos membros do GTTIC) que revelam que nenhum dos requisitos do processo são atendidos, sugerindo uma necessidade de reflexão sobre a oportunidade de melhoria da gestão de riscos em relação ao processo das aquisições de TI na PMF à luz da ISO 31000:2009.

Figura 5 – Visão analítica dos achados da pesquisa

	PROCESSOS	5.2 Comunicação e consulta	5.3 Estabelecimento do contexto	5.4 Avaliação de riscos	5.5 Tratamento de riscos	5.6 Monitoramento e análise crítica	5.7 Registro do processo de gestão de riscos
Membro 1	3 - Aderente	12,50	0,00	0,00	0,00	0,00	0,00
	2 - Parcialmente Aderente	41,67	44,44	22,22	0,00	0,00	0,00
Membro 2	3 - Aderente	62,50	47,57	22,24	0,00	0,00	14,29
	2 - Parcialmente Aderente	25,00	27,08	30,30	36,38	26,67	38,10
Membro 3	3 - Aderente	50,00	41,32	39,30	4,76	40,00	0,00
	2 - Parcialmente Aderente	33,33	34,95	34,34	50,13	40,00	66,67
Membro 4	3 - Aderente	12,50	25,00	0,00	0,00	0,00	0,00
	2 - Parcialmente Aderente	41,67	34,03	0,00	0,00	0,00	0,00
Membro 5	3 - Aderente	0,00	29,17	29,70	0,00	60,00	0,00
	2 - Parcialmente Aderente	50,00	31,02	33,94	17,99	26,67	66,67
Membro 6	3 - Aderente	12,50	3,13	0,00	0,00	0,00	0,00
	2 - Parcialmente Aderente	41,67	39,35	4,44	0,00	0,00	0,00
Membro 7	3 - Aderente	12,50	29,17	26,06	0,00	40,00	0,00
	2 - Parcialmente Aderente	58,33	43,52	21,01	51,85	40,00	66,67
MÉDIA	3 - Aderente	**23,21**	**25,05**	**16,80**	**0,68**	**20,00**	**2,04**
	2 - Parcialmente Aderente	**41,67**	**36,34**	**20,89**	**22,34**	**19,05**	**34,01**

Valores iguais a 0
Valores inferiores o valor final do Q1 (1o. Quartil - 65,25)
Valores maiores que 65,25

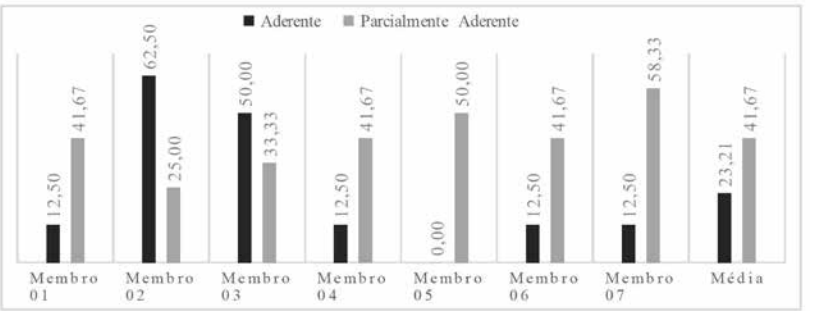
Fonte: pesquisa própria (2023).

É possível verificar na Figura 5 que apenas três valores passaram do valor final do 1º Quartil, encaixando dentro do intervalo do 2º Quartil, o que caracteriza o nível médio de aderência. O valor de referência (66,67) foi indicado pelos membros 3, 5 e 7 no mesmo processo (5.7 – registro do processo de gestão de riscos). Tal valor foi registrado na coluna de 2 – parcialmente aderente. Analisando-se a média de aderência aos processos, para as colunas 3 – aderente e 2 – parcialmente aderente, observa-se um nível de

aderência baixo. A análise de cada um dos processos a partir das respostas dos membros do GTTIC, é particularmente exposta na sequência.

O Gráfico 2 ilustra as respostas dos membros quanto ao nível de aderência do processo 5.2 – Comunicação e consulta.

Gráfico 2 – Nível de aderência ao processo 5.2 – Comunicação e consulta



Fonte: pesquisa própria (2023).

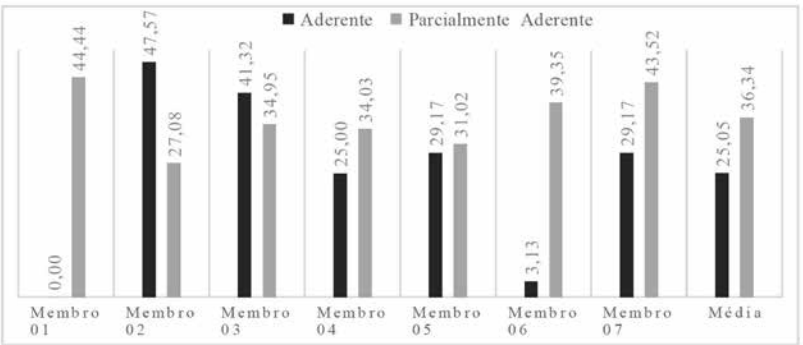
No Gráfico 2, observa-se que a aderência do processo 5.2 – Comunicação e consulta à ISO 31000:2009 assinalou uma média correspondente ao escore de 23,21 para a aderência e 41,67 para a aderência parcial, o que em ambas as medidas equivale a uma baixa aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Destaque-se que, segundo a ABNT (2009), o processo 5.2 – Comunicação e consulta preconiza que em todas as etapas ou atividades do processo de gestão de riscos deve haver uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas.

Verifica-se que os membros do GTTIC que mais utilizam práticas que contribuem para o processo foram os membros 2 e 3, pontuando respectivamente com 62,50 e 50,00. Os demais membros apresentam coincidentemente a mesma pontuação: 12,50. Em linhas gerais, pode-se ponderar que em relação à aderência parcial dos requisitos do processo são utilizadas práticas empíricas para gestão de riscos, que não necessariamente estão alinhadas à ISO 31000:2009. Em resumo, mesmo haven-

do uma maior expressão da aderência parcial, esta ainda se enquadra em baixa aderência pelos valores de referência, indicando que o processo de aquisição da PMF precisa evoluir observando-se os requisitos da norma no tocante ao processo 5.2 – comunicação e consulta.

O Gráfico 3 exibe as respostas dos membros quanto ao nível de aderência do processo 5.3 – Estabelecimento do contexto.

Gráfico 3 – Nível de aderência ao processo 5.3 – Estabelecimento do contexto

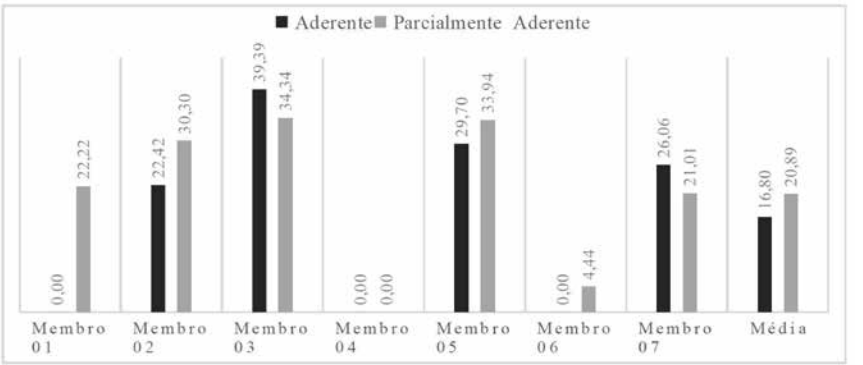


Fonte: pesquisa própria (2023).

No Gráfico 3, é possível notar que a aderência do processo 5.3 – Estabelecimento do contexto obteve média correspondente a 25,05%, o que equivale a uma média aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Segundo a ABNT (2009), o processo 5.3 – Estabelecimento do contexto visa a possibilitar que a organização realize a articulação de seus objetivos, definindo os parâmetros externos e internos a serem considerados no gerenciamento de riscos, e estabelecendo o escopo e os critérios para o restante do processo.

O Gráfico 4 apresenta as respostas dos membros do GTTIC quanto ao nível de aderência do processo 5.4 – Avaliação de riscos.

Gráfico 4 – Nível de aderência ao processo 5.4 – Avaliação de riscos

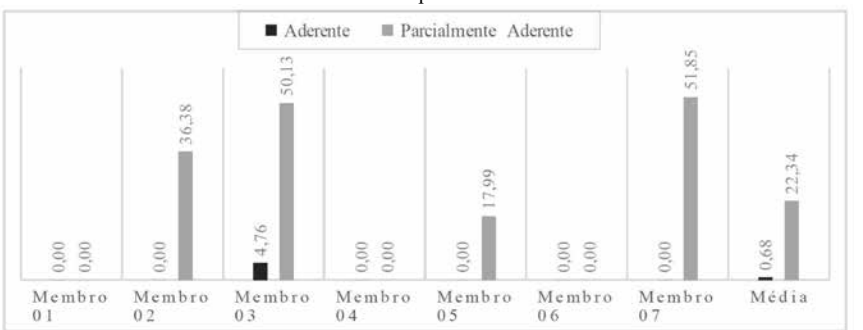


Fonte: pesquisa própria (2023).

Verifica-se que a aderência do processo 5.4 – Avaliação de riscos assinalou média correspondente a 16,8%, o que equivale a uma baixa aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Em linhas gerais, segundo a ABNT (2009), o processo 5.4 – Avaliação de riscos compreende os subprocessos de identificação, análise e avaliação de riscos.

O Gráfico 5 apresenta as respostas dos membros quanto ao nível de aderência do processo 5.5 – Tratamento de riscos.

Gráfico 5 – Nível de aderência ao processo 5.5 – Tratamento de riscos

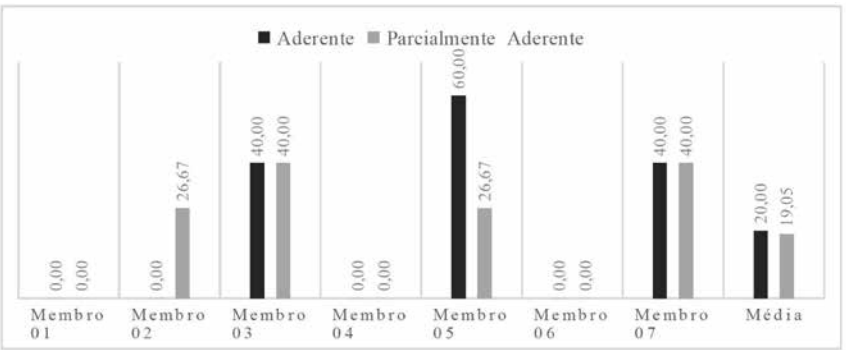


Fonte: pesquisa própria (2023).

No Gráfico 5, é possível notar que a aderência do processo 5.5 – Tratamento de riscos assinalou média correspondente a 0,68%, o que equivale a uma baixa aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Cabe comentar que o processo 5.5 – Tratamento de riscos preocupa-se com a seleção e a implementação de uma ou mais opções para modificar os riscos. Uma vez que haja a implementação, o tratamento fornece novos controles ou realiza a modificação dos existentes (ABNT, 2009).

O Gráfico 6 exibe as respostas dos membros quanto ao nível de aderência do processo 5.6 – Monitoramento e análise crítica.

Gráfico 6 – Nível de aderência ao processo 5.6 - Monitoramento e análise crítica

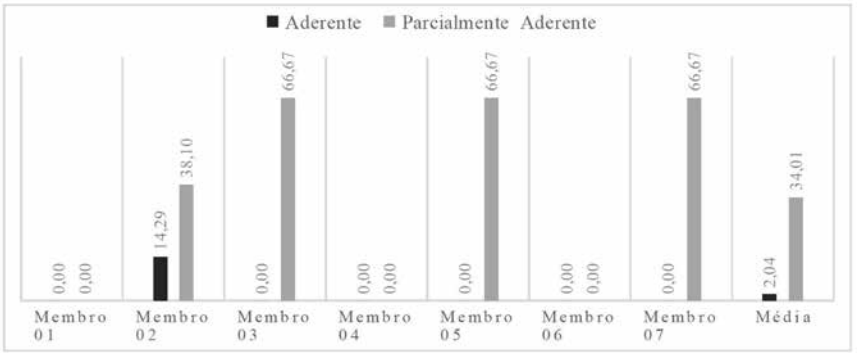


Fonte: pesquisa própria (2023).

No Gráfico 6, é possível perceber que a aderência do processo 5.6 – Monitoramento e análise crítica assinalou média correspondente a 20%, o que equivale a uma baixa aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Segundo a ABNT (2009), o processo 5.6 – Monitoramento e análise crítica sinaliza que o monitoramento e a análise crítica dos riscos sejam planejados como parte da gestão, e envolvam a checagem e o monitoramento regular dos riscos.

O Gráfico 7 ilustra as respostas dos membros quanto ao nível de aderência do processo 5.7 – Registro do processo de gestão de riscos.

Gráfico 7 – Nível de aderência ao processo 5.7 - Registro do processo de gestão de riscos



Fonte: pesquisa própria (2023).

No Gráfico 7, observa-se que a aderência do processo 5.7 – Registro do processo de gestão de riscos assinalou média correspondente a 2,04%, o que equivale a uma baixa aderência, tomando-se como base o escore máximo de aderência segundo a Tabela 2. Ressalte-se que o processo 5.7 – Registro do processo de gestão de riscos sugere que as atividades de gestão de riscos sejam rastreáveis. A geração de registro do processo de gestão de riscos fornece insumos para a melhoria de métodos e ferramentas, bem como de todo o processo (ABNT, 2009).

4.3 Síntese dos resultados da análise de aderência das práticas de gestão de riscos nas aquisições de TI pela PMF

A Tabela 4 apresenta os processos contidos na norma NBR ISO 31000:2009, as proporções dos escores médios obtidos quanto à aderência das práticas de gestão de riscos nas aquisições de TI pela PMF à luz da citada norma, o escore máximo esperado para cada processo e o nível de aderência, conforme descrito na Tabela 2.

Tabela 4 – Nível médio de aderência dos processos das práticas de gestão de riscos nas aquisições de TI pela PMF à luz da ISO 31000:2009

Processo	Proporção média de escores obtida (%)	Valor máximo	Nível médio de aderência
5.2 Comunicação e consulta	23,21	24	Baixo
5.3 Estabelecimento do contexto	25,05	85	Baixo
5.4 Avaliação de riscos	16,80	63	Baixo
5.5 Tratamento de riscos	0,68	54	Baixo
5.6 Monitoramento e análise crítica	20,00	15	Baixo
5.7 Registro do processo de gestão de riscos	2,04	21	Baixo
Total		**262**	

Fonte: pesquisa própria (2023).

Na Tabela 4, é possível uma visão dos resultados obtidos na avaliação realizada junto ao GTTIC tanto de forma geral, como de forma específica para cada processo relacionado às aquisições de TI. Constata-se uma baixa aderência dos processos das práticas de gestão de riscos nas aquisições de TI considerando-se a NBR ISO 31000:2009. Esses resultados divergem dos apontamentos de Munnukka e Järvi (2015) e Santos, Martins e Freitas (2023), que ressaltam que os riscos estão presentes, em diferentes graus, em todos os processos de compras e, por isso, precisam ser gerenciados.

É possível ainda destacar que o processo 5.3 – Estabelecimento do contexto apresenta o maior escore de aderência em relação ao normal, com 25,05%, tendo como objetivo avaliar se durante todas as etapas ou atividades do processo de gestão de riscos ocorre uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas. Assim, a PMF mostra dedicar maior atenção com esse contexto, porém precisa evoluir para o atingimento de todos os requisitos.

Os menores escores obtidos, considerados pontos críticos para o aperfeiçoamento das práticas de gestão de riscos nas aquisições de TI pela PMF,

com 0,68% e 2,04% de aderência à ISO 31000:2009, estão relacionados aos processos 5.5 – Tratamento de riscos e 5.7 – Registro do processo de gestão de riscos. Esses achados vão de encontro à afirmação de Cardoso (2019) de que se torna essencial definir procedimentos práticos e sistematizados que possam ser utilizados para identificar, analisar, avaliar, tratar, monitorar, controlar, documentar e informar riscos nas aquisições de TIC.

Cabe lembrar que Soares (2019) adverte que tratar riscos em aquisições de bens públicos são atividades de controle interno que compreendem processos e atitudes, e pode se fazer uso de algumas técnicas, ações e ferramentas para tal, dentre as quais se destaca a normatização, como a ISO 31000:2009 selecionada como parâmetro da avaliação na pesquisa, sinalizando problemas estruturais nos processos atualmente adotados pela PMF no gerenciamento de riscos nas compras públicas da área de TI.

5 CONSIDERAÇÕES FINAIS

Considerando-se que a nova administração pública incorpora a governança, a gestão de riscos e a integridade, o gerenciamento dos riscos vem ganhando importância na gestão das organizações do setor público, e se apresenta como importante instrumento gerencial para os administradores públicos, em especial para aumentar a segurança e o desempenho das políticas públicas.

Nessa conjunção, para cumprir o objetivo deste artigo, de identificar, à luz da NBR ISO 31000:2009, o nível de aderência de boas práticas de gestão de riscos nas aquisições de TI pela PMF, aplicou-se um questionário estruturado para a coleta de dados primários com o mapeamento dos processos correlatos da NBR ISO 31000:2009. A pesquisa foi respondida por sete dos oito gestores do GTTIC, sendo a aplicação do questionário realizada entre maio e junho de 2022.

No instrumento de avaliação elaborado à luz da NBR ISO 31000:2009, as respostas obtidas foram balizadoras do entendimento do

nível de aderência das práticas em questão e da identificação de possíveis vulnerabilidades para se propor ações de boas práticas.

Em linhas gerais, os achados da pesquisa a partir da percepção dos gestores de TI indicam uma baixa aderência dos processos envolvidos nas práticas de gestão de riscos nas aquisições de TI pela PMF, quer sejam elas empíricas ou formais, contrariando as recomendações da literatura. Os processos e respectivos subprocessos pouco aderentes ou não aderentes à norma NBR ISO 31000:2009 são indicativos da necessidade de revisão das práticas atualmente adotadas na PMF, com destaque para os processos concernentes ao Tratamento de riscos e ao Registro do processo de gestão de riscos.

Por outro lado, foi possível observar algumas iniciativas da PMF de controle dos riscos, mesmo não totalmente aderentes à norma, mas fazendo uso de um direcionamento corporativo para as aquisições de TI, o que demonstra uma preocupação com padronizações, cuidado com redundâncias e uso mais responsável dos recursos públicos.

De qualquer maneira, a partir da percepção dos gestores de TI sobre as práticas de gestão de riscos nas aquisições de TI na PMF, constatou-se que a adoção de tais práticas não é limitante para a tomada de decisão, indo de encontro ao que o TCU (2018a) orienta.

Ademais, destaca-se a relevância dos achados da pesquisa no município de Fortaleza para o avanço do campo de gestão de riscos no setor público a medida em que se considera que eles podem contribuir para o desenvolvimento de práticas mais eficientes e eficazes de gestão de riscos em aquisições de TI em outras organizações públicas. Cardoso (2019) explica que, 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.

Diante do exposto, considera-se que foi possível verificar a aplicabilidade do instrumento de avaliação de aderência das práticas de gestão

de riscos nas aquisições de TI à NBR ISO 31000:2009 na PMF, a partir da percepção do GTTIC. Entretanto, é pertinente ressaltar que, a exemplo da própria norma NBR ISO 31000:2009, o instrumento pode ser utilizado nos mais variados contextos organizacionais, gerando assim uma alternativa para avaliação de aderência e melhoria de práticas de gestão de riscos em organizações do setor público. Assim, espera-se que a pesquisa sirva de base para estudos mais aprofundados acerca do tema, haja vista a relevância do assunto para a sociedade em geral, já que todos são obrigados ao cumprimento das normas, especialmente em função da principal delimitação do presente estudo embrionário que descreveu os resultados dos processos, carecendo de pesquisas com aprofundamento para o nível dos requisitos.

Por fim, e tendo em vista que o estudo suscita questões ainda não resolvidas, por ser limitado à visão do gestor de TI (categoria de sujeitos sociais da presente pesquisa), sugere-se que futuras abordagens venham a considerar a percepção de analistas de segurança da informação, analistas de governança e executivos públicos. Ademais, entende-se que futuras pesquisas podem analisar a adoção de boas práticas de governança sob o olhar da gestão de riscos em outras áreas das organizações públicas. Outra possibilidade de novos estudos sobre o tema é a utilização da nova versão da ISO 31000:2018, permitindo uma verificação de aderência e atualização do instrumento de coleta.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO 31000:2009:** Gestão de riscos – Princípios e diretrizes. 32 f. Rio de Janeiro, 2009.

ÁVILA, M. D. G. Gestão de riscos no setor público. **Revista Controle**: doutrina e artigos, v. 12, n. 2, p. 179-198, 2014.

BITENCOURT, C. F. A importância da informação no contexto da sustentabilidade: uma inovação para maior competitividade nas diretrizes de gestão de risco. **Revista Inteligência Competitiva**, v. 9, n. 4, p. 1-14, 2019.

CARDOSO, F. F. **GRATIC**: uma metodologia para gestão de riscos em aquisições de TIC no âmbito dos institutos federais de educação. 2019. 189 f. Dissertação (Mestrado Profissional em Ciência da Computação) – Centro de Informática, Universidade Federal de Pernambuco (UFPE), Recife, 2019.

CARDOSO, F. F.; ALVES, C. F. GRATIC: uma metodologia para gestão de riscos em aquisições de TIC. *In*: Workshop de Computação Aplicada em Governo Eletrônico: Congresso da Sociedade Brasileira de Computação (CSBC), 8, 2020. Cuiabá. **Anais**... Cuiabá: CSBC, 2020. p. 36-47.

FERNANDES, F. C.; KROENKE, A.; SÖTHE, A. Uma visão atual do processo de controle e gerenciamento de riscos operacionais nos 10 maiores bancos brasileiros. *In*: Seminários em Administração FEA/USP – Semead, 12, 2009. **Anais**... São Paulo: USP, 2009. p. 1-16.

FORTALEZA (CE). **Lei Complementar nº 176, de 19 de dezembro de 2014**. Dispõe sobre a organização e a estrutura administrativa do Poder Executivo Municipal e dá outras providências. Diário Oficial do Município, 19 de dezembro de 2014. Disponível em: https://planejamento.fortaleza.ce.gov.br/images/Legislacao/reforma_etapadois.pdf. Acesso em: 27 abr. 2022.

FORTALEZA (CE). **Decreto nº 13.566 de 7 de abril de 2015**. Dispõe sobre a criação do Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação no âmbito do Município de Fortaleza, e dá outras providências. Disponível em: https://planejamento.fortaleza.ce.gov.br/images/redes_corporativas/ti/DOM_15500_Publicao-do-Decreto-SISTIC.pdf. Acesso em: 1 maio 2022.

FORTALEZA (CE). **Instrução Normativa nº 002/2019-SEPOG, de 24 de janeiro de 2019**. Estabelece regras acerca dos procedimentos relacionados aos serviços de nuvem oferecidos pelo data center corporativo da administração pública municipal e dá outras providências. Disponível em: https://planejamento.fortaleza.ce.gov.br/images/redes_corporativas/ti/DOM_16.455_IN_de_Uso_do_Data_Center.pdf. Acesso em: 7 maio 2022.

FREITAS, H. *et al*. O método de pesquisa survey. **Revista de Administração da Universidade de São Paulo – RAUSP**, v. 35, n. 3, p. 105-112, 2000.

GARCEZ, L. R. S. **Análise da gestão de riscos na área de compras da Fiocruz**. 2019. 113 f. Dissertação (Mestrado em Saúde Pública) – Escola Nacional de Saúde Pública Sergio Arouca, Fundação Oswaldo Cruz, Rio de Janeiro, 2019.

JUNQUEIRA, F. A. **A influência do processo de gestão de riscos da ABNT NBR ISO 31000-2018 na tomada de decisão**: um estudo com profissionais de saúde e segurança do trabalho. 2021. 301 f. Dissertação (Mestrado Profissional em Administração) – Fundação Cultural Dr. Pedro Leopoldo – FPL, Pedro Leopoldo, 2021.

KELLER, C.; KÖHLER, M. Risk assessment of technology trends in supply chain management. **Journal of Supply Chain and Operations Management**, v. 19, n. 2, p. 128-152, 2021.

KLEIN JUNIOR, V. H. Gestão de riscos no setor público brasileiro: uma nova lógica de accountability?. **Revista de Contabilidade e Organizações**, v. 14, p. e163964-e163964, 2020.

MARTIN, N. C.; SANTOS, L. R. D.; DIAS FILHO, J. M. Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria. **Revista Contabilidade & Finanças**, v. 15, p. 7-22, 2004.

MORAES, M. E. L. B. N. O. **Gestão de riscos no âmbito da administração pública do Distrito Federal**. 2020. 131 f. Dissertação (Mestrado Profissional em Administração Pública) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2020.

MOURÃO, A.; MARINHO, S. V. Análise do desempenho do processo de compras em uma empresa pública de pesquisa. **Gestão & Regionalidade**, v. 38, n. 114, p. 327-344, 2022.

MUNNUKKA, J.; JÄRVI, P. The influence of purchase-related risk perceptions on relationship commitment. **International Journal of Retail & Distribution Management**, v. 43, n. 1, p. 92-108, 2015.

NISHIYAMA, M. A.; LIMA, M. V, A.; ENSSLIN, L.; CHAVES, L. Modelo multicritério para avaliação de desempenho: um estudo de caso para gestão de compras no setor público. **Revista de Ciências da Administração**, v. 19, n. 47, p. 9-28, 2017.

NOBRE, L. S. **Proposta de metodologia de gestão de riscos para as contratações de TI da Funasa**. 2017. 112 f. Dissertação (Mestrado Profissional em Computação Aplicada) – Universidade de Brasília, Brasília, 2017.

OLIVEIRA, U. R. *et al*. The ISO 31000 standard in supply chain risk management. **Journal of Cleaner Production**, v. 151, p. 616-633, 2017.

PARREIRA, G. C. **Modelo de decisão para gestão de riscos de contratos de serviços de TI no poder judiciário brasileiro**. 2018. 92 f. Dissertação (Mestrado Profissional em Computação Aplicada) – Universidade de Brasília, Brasília, 2018.

PENHA, J. C.; PARISI, C. Um caminho para integrar a gestão de riscos à controladoria. *In*: Congresso Brasileiro de Custos, 12, 2005. **Anais**... Florianópolis: ABC, 2005. p. 1-15.

PIRES, T. G.; CAVALCANTE, S. M.; CORREA, D. M. M. C. Gestão de riscos nas aquisições de soluções de TI: uma análise crítica dos modelos de boas práticas. *In*: Eati – Encontro Anual de Tecnologia da Informação e Stin – Simpósio de Tecnologia da Informação da Região Noroeste do RS, 6, 2016. **Anais**... Frederico Westphalen/RS: Eati, 2016. p. 93-100.

SANTOS, A. C. C. **Gestão de riscos**: avaliação de riscos operacionais em uma empresa de serviço de entrega de encomendas. 2017. 77 f. Dissertação (Mestrado em Administração) – Unifacs, Universidade Salvador, Salvador 2017.

SANTOS, L. F. M. D.; MARTINS, R. S.; FREITAS, J. S. Configurações explicativas do desenvolvimento da resiliência nas redes de suprimentos da administração pública. **Revista de Administração Pública**, v. 57, n. 1, p. 1-22, 2023.

SANTOS, T. J. Gestão de riscos e a norma ISO 31000: uma abordagem literária. **Management Journal**, v. 3, n. 1, p. 1-14, 2021.

SCANNELL, T.; CURKOVIC, S.; WAGNER, B. Integration of ISO 31000:2009 and supply chain risk management. **American Journal of industrial and Business Management,** v. 3, n. 4, p. 367-377, 2013.

SILVA, D. A.; OLIVEIRA, E. C.; CANEDO, E. D. Avaliação de riscos do processo de planejamento da contratação de TI: uma proposta para órgãos governamentais brasileiros. **Revista Brasileira de Sistemas de Informação**, v. 9, n. 1, p. 168-186, 2016.

SILVA JÚNIOR, S. D.; COSTA, F. J. Mensuração e escalas de verificação: uma análise comparativa das escalas de Likert e Phrase Completion. **PMKT – Revista Brasileira de Pesquisas de Marketing, Opinião e Mídia**, v. 15, n. 1-16, p. 61, 2014.

SOARES, J. C. A. **Gestão de riscos em compras públicas**: um estudo na Central de Compras do Estado da Paraíba. 2019. 140 f. Dissertação (Mestrado em Gestão Pública e Cooperação Internacional) – Universidade Federal da Paraíba, João Pessoa, 2019.

SOARES NETTO, A. F. **Proposta de artefato de identificação de riscos nas contratações de TI da administração pública federal, sob a ótica da ABNT NBR ISO 31000** – gestão de riscos. 2013. 133 f. Dissertação (Mestrado em Engenharia Elétrica) – Departamento de Engenharia Elétrica, Faculdade de Tecnologia, Universidade de Brasília, Brasília, 2013.

TCU. Tribunal de Contas de União. **Referencial básico de gestão de riscos**. SEGECEX/COGER. Brasília, DF: TCU, 2018a. Disponível em: https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE-6F18818A8/Referencial_basico_gestao_riscos.pdf. Acesso em: 28 jul. 2023.

TCU. Tribunal de Contas de União. **Relatório técnico completo de acompanhamento IGG 2018**. Brasília, DF: TCU, 2018b. Disponível em: https:// portal.tcu.gov.br. Acesso em: 28 jul. 2023.

TERRA, A. C. P. Compras públicas inteligentes: Uma proposta para a melhoria da gestão das compras governamentais. **Revista de Gestão Pública**, v. 1, n. 1, p. 46-70, 2018.

TRIVELATO, B. F.; MENDES, D. P.; DIAS, M. A. A importância do gerenciamento de riscos nas organizações contemporâneas. **Revista Fatec Zona Sul**, v. 4, n. 2, p. 1-20, 2018.

VIEIRA, J. B.; BARRETO, R. T. D. S. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019. 240 p. Disponível em: http://repositorio.enap.gov.br/handle/1/4281. Acesso em 15 abr. 2022.

WALRAVEN, A. L. *et al*. Análise da implantação da gestão de riscos na unidade de auditoria interna do Tribunal de Justiça do estado do Ceará. **Revista Controle**: doutrina e artigos, v. 21, n. 1, p. 136-173, 2023.