ISSN: 2359-1048
Novembro 2022

GESTÃO DE RISCOS À LUZ DA NBR ISO 31000: uma análise das aquisições de tecnologia da informação da Prefeitura Municipal de Fortaleza

ALEXSANDRO ARAÚJO DA SILVA
UNIVERSIDADE FEDERAL DO CEARÁ - UFC

MARIÂNGELA ARAUJO PINTO BEZERRA

JORGE ALBERTO CAVALCANTI ALCOFORADO
UNIVERSIDADE FEDERAL DO CEARÁ - UFC

AIRTON DOUGLAS DE ANDRADE LUCAS
UNIVERSIDADE DE FORTALEZA - UNIFOR

ALESSANDRA CARVALHO DE VASCONCELOS

Introdução
O 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 TIC na Prefeitura Municipal de Fortaleza. Tem-se a intenção de que à luz da norma ISO 31000 se possa identificar o nível da aderência das decisões tomadas sobre aquisições de TIC na organização estudada. Os resultados poderão apoiar gestores públicos, na tomada de decisões das aquisições de TIC, sendo possível sua aplicação para outros aspectos da governança pública que envolvem riscos.
Problema de Pesquisa e Objetivo
À luz da ISO 31000, 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? Assim, o objetivo geral do presente artigo é analisar, à luz da ISO 31000, a aderência de boas práticas de gestão de riscos nas aquisições de tecnologia da informação na Prefeitura Municipal de Fortaleza.
Fundamentação Teórica
No contexto da governança, a gestão de riscos pode ser vista como o processo que trata da criação, distribuição e preservação de valor para as organizações (Vieira & Barreto, 2019). Ademais, conforme a norma ABNT NBR 31000 (2009), gerenciar riscos é parte da governança e liderança, e é fundamental para a maneira como a organização é gerenciada em todos os níveis, contribuindo para a melhoria dos sistemas de gestão. Desta forma, a norma ISO 31000 pode ser aplicada a qualquer tipo de risco e em qualquer segmento de organizações (Santos, 2021).
Metodologia
Para o alcance do objetivo da pesquisa descritiva, o estudo de caso único, de natureza qualitativa, foi aplicado um questionário junto aos representantes do Grupo Técnico de TIC da Prefeitura Municipal de Fortaleza (PMF), no período de 20 de maio a 03 de junho de 2022. A estruturação do questionário tomou como base a NBR ISO 31000:2009 e adotou a escala tipo Likert para cada processo da ISO 31000. Para a análise do nível de aderência das práticas de gestão de riscos nas aquisições de tecnologia da informação na PMF à luz da ISO 31000 foi utilizada a análise dos quartis.
Análise dos Resultados
A partir da avaliação realizada junto ao Grupo Técnico de TIC da Prefeitura de Fortaleza, constata-se que há baixa aderência dos processos das práticas de gestão de riscos nas aquisições de TI considerando a norma ISO 31000. De forma mais pontual, foi possível verificar que o processo que apresenta o maior percentual de aderência em relação à norma, com 25,05%, é o Estabelecimento do contexto, e que os processos com os menores percentuais de aderência à ISO 31000 são Tratamento de riscos e Registro do processo de gestão de riscos, respectivamente.
Conclusão
Os resultados apontam importante vulnerabilidade dos processos da Prefeitura de Fortaleza relacionados às práticas de gestão de riscos nas aquisições de TI, quer sejam elas empíricas ou formais. Os processos e respectivos subprocessos pouco aderentes ou não aderentes à ISO 31000 são indicativos de revisão das práticas atualmente adotadas na Prefeitura, com destaque aos processos concernentes ao Tratamento de riscos e ao Registro do processo de gestão de riscos. Conclui-se que há baixa aderência dos processos das práticas de gestão de riscos nas aquisições de TI considerando a ISO 31000.
Referências Bibliográficas
ABNT - Associação Brasileira de Normas Técnicas. NBR 31000: Gestão de riscos - Princípios e diretrizes. Rio de janeiro, 2009. Recuperado de https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em: 03 mar. 2022. Santos, T. J. (2021). Gestão de riscos e a norma ISO 31000: uma abordagem literária. Management Journal 3(1), 1-14. Vieira, J. B., & Barreto, R. T. D. S. (2019). Governança, gestão de riscos e integridade. Brasília: Enap. 240 p. Recuperado de http://repositorio.enap.gov.br/handle/1/4281. Acesso em: 06 maio 2022.

Palavras Chave
Governança pública, Gestão de riscos, NBR ISO 31000

GESTÃO DE RISCOS À LUZ DA NBR ISO 31000: uma análise das aquisições de tecnologia da informação da Prefeitura Municipal de Fortaleza

1 INTRODUÇÃO

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 da Prefeitura Municipal de Fortaleza.

No caminho de uma governança pública em prol da sustentabilidade, Moraes (2020) afirma que o gerenciamento de riscos vem ganhando importância na gestão das organizações do setor público. A partir de experiências exitosas no manejo de incertezas a que estão sujeitas quaisquer organizações, a gestão de riscos no âmbito público se apresenta como importante instrumento gerencial para os administradores públicos, em especial, para aumentar a segurança e o desempenho na consecução das políticas públicas.

Garcez (2019) reforça que, no entanto, 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 que risco é o efeito da incerteza sobre os objetivos. Esse efeito, no caso, é um desvio em relação ao esperado, e pode ser positivo ou negativo. O Brasil, de acordo com parâmetros internacionais, por meio da Agência Brasileira de Normas Técnicas (ABNT), publicou a ABNT NBR ISO 31000 Gestão de Riscos - Princípios e Diretrizes, que registra o mesmo conceito.

Com um enfoque mais específico, Parreira (2018) alerta que as aquisições que envolvem TIC geralmente são complexas e burocráticas, exigindo conhecimento técnico aprofundado no assunto, além de competências para planejar e gerir adequadamente a contratação, de acordo com a legislação vigente. No mesmo sentido, Pires (2016) afirma que as incertezas geradas por problemas financeiros, recursos humanos e tecnológicos trazem diversos riscos e inseguranças para os gestores e em muitos casos causam interrupções no processo licitatório e atrasos em entregas.

Para Martin, Santos e Dias (2004), a Controladoria tem como uma de suas funções, as atividades de identificar, mensurar, analisar, avaliar, divulgar e controlar os diversos riscos envolvidos no negócio, bem como seus possíveis efeitos. Nesse contexto, a Prefeitura Municipal de Fortaleza (PMF), através da Secretaria de Planejamento e Gestão (SEPOG), criou o Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação (SETIC), regulamentado através do Decreto nº 13.566, de 07 de abril de 2015, que tem como função a tomada de decisão no âmbito da TIC.

Através do SISTEC, foi definido, por meio da Instrução Normativa da SEPOG Nº 002, de 24 de janeiro de 2019, um novo método de aquisição de TIC na PMF (Fortaleza, 2019), onde se definiu que toda aquisição de TIC da prefeitura fosse submetida a uma análise prévia. Com essa ação, a PMF projeta uma diminuição da possibilidade de problemas, seja de conformidade, *compliance* ou simplesmente fora de diretrizes pré-definidas.

Conforme Fernandes, Kroenke e Söthe (2009), o controle focado na gestão de riscos operacionais é fundamental para prever, classificar e mitigar os riscos presentes em todas as decisões. Isso pode mitigar a probabilidade de eventos inesperados e outras perdas resultantes de riscos não calculados. É importante que este controle seja realizado por uma equipe especializada, ou seja, que não possua outras atividades além do controle de riscos operacionais na instituição, pois é um trabalho complexo e de grande responsabilidade (Fernandes, Kroenke, & Söthe, 2009).

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, a demanda por normas, metodologias e ferramentas capazes de lidar com os riscos tornou-se fundamental.

Diante da importância da temática para as organizações públicas, o estudo de Netto (2013), aplicado no âmbito federal, fez uso da ISO 31000 nas contratações de TI. O estudo propôs uma ferramenta focada especificamente na identificação de riscos e serviu como fator motivador para este trabalho. Assim, esta pesquisa empírica, aplicada especificamente no âmbito municipal, busca preencher a lacuna de analisar as contratações de TIC com um olhar mais amplo, perpassando por todos os processos da ISO 31000, não direcionado exclusivamente para a identificação de riscos.

Segundo Bitencourt (2019), uma das preocupações da sustentabilidade no contexto das organizações é a gestão de riscos, 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 para grandes desafios e muitos riscos. Nesse contexto, a governança corporativa, o *compliance* e a gestão de riscos são disciplinas obrigatórias como ferramentas de gestão (Trivelato, Mendes, & Dias, 2018).

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 Silva (2016), Nobre (2017) e CGU (2018), não foi percebido uma análise estruturada e comparativa com a ISO 31000, através de um instrumento, como é a proposta deste trabalho. A maioria dos estudos empíricos se concentra no planejamento das aquisições. Segundo Netto (2013), para tratar essa lacuna é necessário um apoio metodológico ou procedimental. Desta forma, é possível a utilização da gestão de riscos baseado na norma ABNT NBR 31000, cuja utilização pode ser destinada às contratações de TIC, haja visto que o gerenciamento de riscos tem sido utilizado por organizações de diversos segmentos devido a sua aplicação multidisciplinar.

Instrumentos que possam assessorar gestores de TIC a controlar os riscos nos processos de aquisição passam a ser fundamentais. Segundo Cardoso (2019), é dito que além da complexidade inerente aos processos da TIC, a rotatividade dos atores envolvidos no processo e as particularidades de cada equipe de planejamento da contratação, é importante 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.

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

A análise resultante da aplicação do instrumento de avaliação na PMF poderá permitir associar riscos, decisões e entender as pressões que levam os tomadores de decisão, mais especificamente da área de TIC na PMF nas questões norteadoras, éticas e ambientais em seus modelos de negócio.

Ao desenvolver a pesquisa, tem-se a intenção de que à luz da ISO 31000 se possa 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 à tomada de decisões no que tange a aquisições de TI, com a possibilidade de expandir para outros aspectos da governança que envolvem riscos. Ressaltando, que no primeiro momento, o

instrumento de avaliação adotado nesta pesquisa poderá ser replicado na própria PMF, foco desta pesquisa, e em outros entes públicos.

2 PROBLEMA DE PESQUISA E OBJETIVO

À luz da ISO 31000, 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?

Assim, o objetivo geral do presente artigo é analisar, à luz da ISO 31000, a aderência de boas práticas de gestão de riscos nas aquisições de tecnologia da informação na Prefeitura Municipal de Fortaleza.

3 REVISÃO DE LITERATURA

3.1 Gestão de riscos e a ABNT NBR ISO 31000

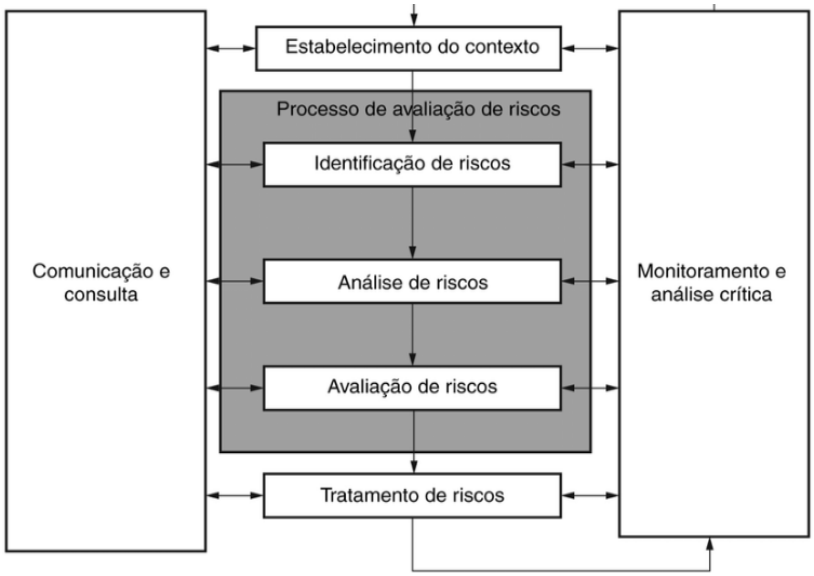
O conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos é denominado de gestão de riscos. Dependendo do porte e da complexidade das operações, organizações adotam abordagens informais, bem como, estruturadas e sistematizadas, para gestão de riscos visando alcançar 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 atenção, contudo, este assunto não é novo. Sob o olhar de controles internos, a auditoria interna contribui para gestão de riscos (Penha & Parisi, 2005).

A gestão de riscos tem a responsabilidade de implantar um processo de administração eficiente e continuado nas organizações, visando a melhoria contínua através da redução de prejuízos e aumento dos benefícios, porém, existe a necessidade de uma padronização de conceitos, pressupostos, regulamentações e *frameworks*, que auxilie as organizações a gerirem de forma eficiente, eficaz e coerentemente os seus riscos. Nesse sentido, a norma ISO 31000:2009 foi desenvolvida originalmente pela International Organization for Standardization (ISO) e contou com a participação de especialistas de mais de 30 países. Desta forma, a ISO 31000 pode ser aplicada a qualquer tipo de risco e em qualquer segmento de organizações (Santos, 2021).

Já a ABNT NBR ISO 31000 foi elaborada na Comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-063). O projeto circulou em consulta nacional conforme Edital nº 02, de 07 de fevereiro de 2018 a 08 de março de 2018. Esta norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 31000:2018, que foi elaborada pelo Technical Committee Risk Management (ISO/TC 262), conforme ISO/IEC Guide 21-1:2005. Organizações de todos os tipos e tamanhos enfrentam influências e fatores externos e internos que tornam incerto se elas alcançarão seus objetivos.

Gerenciar riscos é parte da governança e liderança, e é fundamental para a maneira como a organização é gerenciada em todos os níveis, contribuindo para a melhoria dos sistemas de gestão. Gerenciar riscos é parte de todas as atividades associadas com uma organização e inclui interação com as partes interessadas e deve considerar os contextos externo e interno da organização, incluindo o comportamento humano e os fatores culturais (ABNT NBR 31000, 2009). Em suma, gerenciar riscos baseia-se nos princípios, estrutura e processos delineados neste documento, conforme descrito na Figura 1.



Fonte: Adaptado de ABNT NBR 31000 (2009).

Figura 1. Processo de gerenciamento de riscos

Do exposto na Figura 1, convém que o processo de gestão de riscos seja parte integrante da gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização. Pode ser aplicado nos níveis estratégico, operacional, de programas ou de projetos, sendo possível muitas aplicações do processo de gestão de riscos personalizadas para alcançar 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 31000:2018, é importante que a natureza dinâmica e variável do comportamento humano e a cultura sejam consideradas. 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.

Diante da relevância da temática, alguns estudos empíricos sobre o assunto foram desenvolvidos. A seguir, as pesquisas mais correlatas são brevemente descritas.

3.2 Estudos empíricos anteriores

A Figura 2 apresenta de forma sucinta alguns estudos empíricos nacionais e internacionais que assim como a presente pesquisa, investigaram, amparados na ISO 31000, a gestão de riscos e a gestão de aquisições de TIC em diferentes contextos organizacionais.

Autoria	Objetivos	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 dos profissionais.	Propor um quadro abrangente para o risco de avaliação de novas tecnologias em oferta da gestão da cadeia. Para tanto, foram usadas metodologias existentes, especialmente seis metodologias de avaliação de risco, 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 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 através de um inventário de riscos, 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 aquisições de TI da Fundação Nacional de Saúde (FUNASA).	Os resultados demonstram que a metodologia proposta apresenta viabilidade para sua utilização nos órgãos públicos federais como meio de auxiliar a internalização de procedimentos previstos na legislação e o aprofundamento do tema de gestão de riscos nas contratações de TI na Administração Pública Federal (APF).
Netto (2013)	Desenvolver um artefato para a identificação de riscos para o processo de contratação de TI na APF, sob o ponto de vista da Norma 31000.	Constatou-se que, com o uso do artefato, os gestores podem encontrar vulnerabilidades que antes não eram possíveis de serem observadas, o que permitirá uma melhoria na definição dos níveis de serviço e na gestão contratual, por meio de uma construção mais eficaz do termo de referência. Os resultados demonstram que o artefato servirá como uma fonte consolidada de informação para identificação de riscos nas contratações de TI na APF.
Scannell, Curkovic e Wagner (2013)	Determinar se a ISO 31000 fornece a estrutura para chegar a um consenso sobre o escopo e a definição da SCRM, o que, por sua vez, pode acelerar a pesquisa da SCRM, e examinar se a ISO 31000 fornece a base para o planejamento e execução da SCRM.	Verificou-se que as empresas reconhecem a importância da Gestão de Riscos na Cadeia de Suprimentos (SCRM), mas falta integração e habilidades da SCRM.

Fonte: Elaborado pelos autores.

Figura 2. Estudos empíricos anteriores

As informações evidenciadas na Figura 2, que descrevem os objetivos e os principais achados dos estudos correlatos identificados na revisão de literatura, ressaltam a relevância da presente pesquisa por (i) considerar todos os processos da ISO 31000 para a avaliação de aderência através de um instrumento de verificação e (ii) sua utilização no âmbito de uma prefeitura.

4 METODOLOGIA

A pesquisa descritiva foi realizada por meio da obtenção de dados primários, com o intuito de identificar o nível de aderência da gestão de riscos nas aquisições de tecnologia da informação na Prefeitura Municipal de Fortaleza (PMF), observando as orientações normativas da ISO 31000.

O questionário foi estruturado no formato de um *checklist* e aplicado junto aos oito representantes do Grupo Técnico de TIC da PMF no período de aplicação da pesquisa, que corresponde a 20 de maio a 03 de junho de 2022. Nesse sentido, o resultado do preenchimento do questionário possui o intuito de descrever a situação atual, em termos de aderência com ferramentas de boas práticas de gestão de riscos, e contribui com um modelo comparativo, podendo ser replicado, com as devidas adaptações, a outras realidades em outros entes da gestão pública.

A avaliação resultante da aplicação do questionário junto ao Grupo Técnico de TIC da PMF permitirá associar riscos, decisões e entender as pressões que levam os tomadores de decisão da área de TI na PMF nas questões norteadoras, éticas e ambientais em seus modelos de negócio.

Cabe informar que a estruturação do questionário tomou como base a NBR ISO 31000:2009, que está segmentada em três partes: 1 - princípios e diretrizes, 2 - estrutura e 3 - processo. Das três partes citadas, no estudo, é dado destaque à parte do processo, que é identificada no item 5 na norma. Dentro deste item, foram considerados no questionário os

processos e subprocessos, a quantidade de requisitos e o escore máximo de cada um, conforme exposto na Tabela 1.

Tabela 1. Estruturação da pesquisa segundo os processos da ISO 31000

Processos	Quantidade 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**	**261**

Fonte: Elaborado pelos autores.

Destaca-se que os processos da ISO 31000 que foram base de avaliação da aderência na pesquisa são divididos em subprocessos, a saber: O processo 5.3, que é o 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 risco. O processo 5.4, que é a avaliação de riscos, é dividido em 3 subprocessos, 5.4.1 - identificação de riscos, 5.4.2 - análise de riscos, 5.4.3 - avaliação de riscos. O processo 5.5, que é o tratamento de riscos, é dividido em 3 subprocessos, 5.5.1 - Generalidade, 5.5.2 - seleção das opções de tratamento de riscos, 5.5.3 - preparando e implementando planos para tratamento de riscos.

Conforme pode ser visto no escore máximo atribuído na Tabela 1, foi realizada uma adaptação da escala tipo Likert para cada processo da ISO 31000 no questionário, sendo usado os seguintes parâmetros de verificação: Aderente, Parcialmente aderente e Não aderente, cujos valores numéricos atribuídos foram respectivamente 3, 2 e 1. Foi utilizado também o parâmetro Não se aplica, com valor 0, para sinalização de não utilização do processo ou subprocesso. O escore máximo que consta na Tabela 1 foi atribuído levando-se em consideração a completude de todos os requisitos de um processo, multiplicado pelo valor máximo de aderência que é 3, conforme descrito anteriormente.

Para a realização da avaliação do nível de aderência das práticas de gestão de riscos nas aquisições de tecnologia da informação na PMF à luz da ISO 31000, foi utilizada a análise dos quartis. O nível máximo de aderência corresponde a 261 pontos, baseado na utilização de todos os critérios de todos os processos. A ponderação utilizada pode ser vista na Tabela 2 (tabela de referência).

Tabela 2. Análise do nível de aderência baseado em quartis

Quartil	Valor inicial	Valor final	% máximo de aderência	Nível de aderência
Q1	0,00	65,25	25,00%	Baixa aderência
Q2	65,26	130,50	50,00%	Média aderência
Q3	130,60	195,80	75,00%	Aderente
Q4	195,90	261,00	100,00%	Forte aderência

Fonte: Elaborado pelos autores.

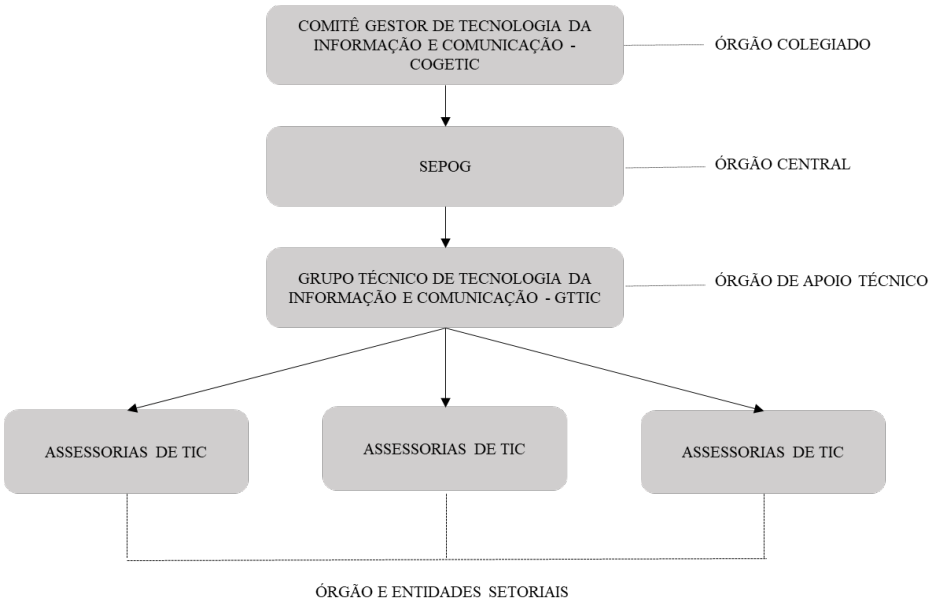
5 RESULTADOS E DISCUSSÃO

5.1 Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação

Antes de descrever os resultados da avaliação do nível de aderência das práticas de gestão de riscos nas aquisições de tecnologia da informação na PMF, cabe apresentar brevemente a estrutura do Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação (SISTIC) do município de Fortaleza.

Criado por meio do Decreto nº 13.566, de 07 de abril de 2015, o Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação (SISTIC) compreende as atividades de planejamento, governança, coordenação, organização, aquisição, operação, controle e supervisão dos recursos de tecnologia da informação e comunicação dos órgãos e entidades da administração pública municipal (Decreto nº 13.566, 2015).

A Figura 3 apresenta a estrutura do SISTIC, que é o sistema gestor de tecnologia da informação da Prefeitura Municipal de Fortaleza (PMF).

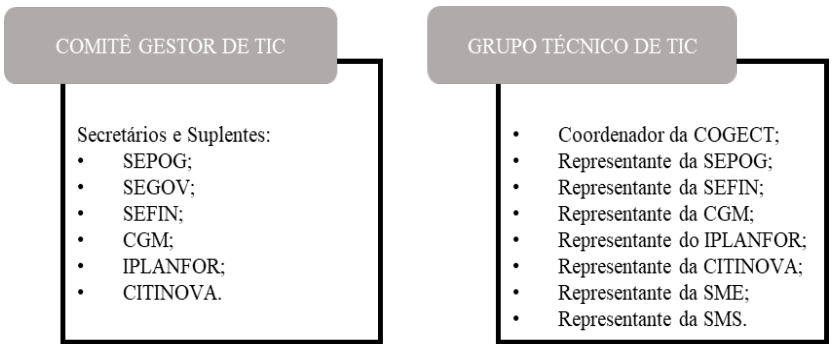


Fonte: Elaborada pelos autores.

Nota: Secretaria Municipal do Planejamento, Orçamento e Gestão (SEPOG).

Figura 3. Estrutura do SISTIC da PMF

A estrutura do SISTIC visa tomar decisões estratégicas no âmbito da Prefeitura Municipal de Fortaleza, no tocante aos ativos e soluções de TIC. A Figura 4 apresenta a composição do SISTIC.



Fonte: Elaborada pelos autores.

Nota: 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); Secretaria Municipal da Saúde (SMS).

Figura 4. Composição do SISTIC da PMF

A Figura 4 apresenta os componentes do SISTIC, que é formado pelo Comitê Gestor de TIC, composto pelos secretários e suplentes da 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) e pelo grupo técnico de TIC, composto pelo coordenador da Coordenadoria de Gestão Corporativa de Tecnologia da Informação (COGECT), pelos representantes da Secretaria Municipal do Planejamento, Orçamento e Gestão (SEPOG), 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), Secretaria Municipal da Saúde (SMS) e da Secretaria Municipal da Educação (SME).

Após esta breve descrição sobre a estrutura e a composição do Sistema Municipal de Gestão da Tecnologia da Informação e Comunicação (SISTIC) do município de Fortaleza, a seguir são apresentados os resultados da avaliação da aderência das práticas de gestão de riscos nas aquisições de TI tendo como parâmetro os processo da norma ABNT NBR 31000.

5.2 Nível de aderência das práticas de gestão de riscos nas aquisições de TI na PMF

Os resultados da pesquisa quanto à análise do nível de aderência das práticas de gestão de riscos nas aquisições de TI na Prefeitura de Fortaleza correspondem às respostas do questionário obtidas junto a sete dos oito representantes do Grupo Técnico de TIC da PMF. O questionário foi aplicado no período de 20 de maio a 03 de junho de 2022.

Para a análise do nível de aderência foram considerados todos os 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 e 5.7 Registro do processo de gestão de riscos), evidenciados na Tabela 1, com seus respectivos subprocessos. O nível máximo de aderência corresponde a 261 pontos, baseado na utilização de todos os critérios de todos os processos da ISO 31000, sendo a ponderação feita por meio dos quartis (Tabela 2).

Do 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 tecnologia da informação na Prefeitura de Fortaleza à luz da ISO 31000, 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.

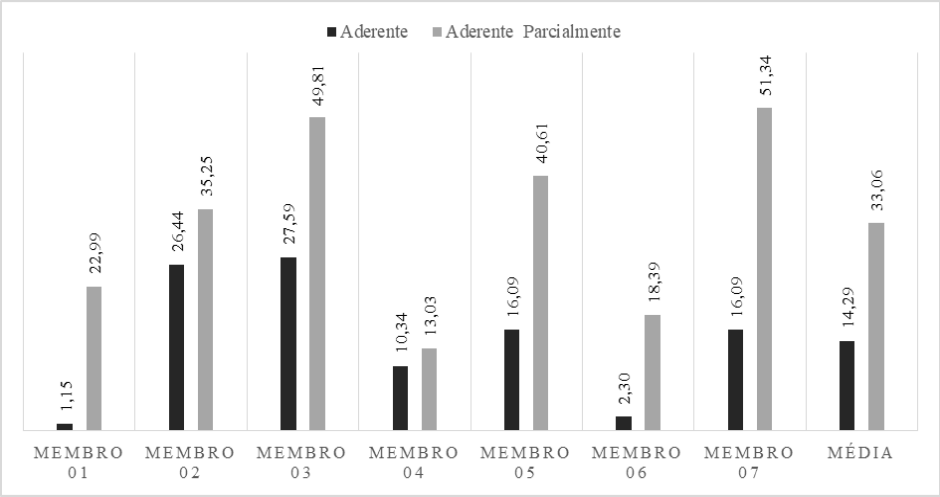
Tabela 3. Exemplo do instrumento de apuração de aderência - NBR ISO 31000:2009

Processo 5.2 Comunicação e consulta		**Escala**		
Objetivo	**Requisito**	**Aderente**	**Parcialmente aderente**	**Não aderente**
Durante todas as etapas ou atividades do processo de gestão de riscos deve haver uma efetiva comunicação	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 em conjunto para análise dos riscos?	3		

informativa e consultiva entre a organização e as partes interessadas, internas e externas. Avalie as questões alusivas ao processo da Comunicação e Consulta relacionado aos riscos:	5. Os diferentes pontos de vista são devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos?	3		
	6. É dado o aval e o apoio 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 interna e externa?		2	
Nível de aderência do processo 5.2 identificado = 20 (ou 83,33%)		**12**	**8**	
Nível de máximo de aderência do processo 5.2 = 24 (ou 100,00%)		**24**		

Fonte: Elaborado pelos autores.

O resultado geral das respostas dos membros participantes do Grupo Técnico de TIC quanto à aderência dos 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 e 5.7 Registro do processo de gestão de riscos) relacionados às práticas de gestão de riscos nas aquisições de tecnologia da informação na Prefeitura de Fortaleza está apresentado na Figura 5.

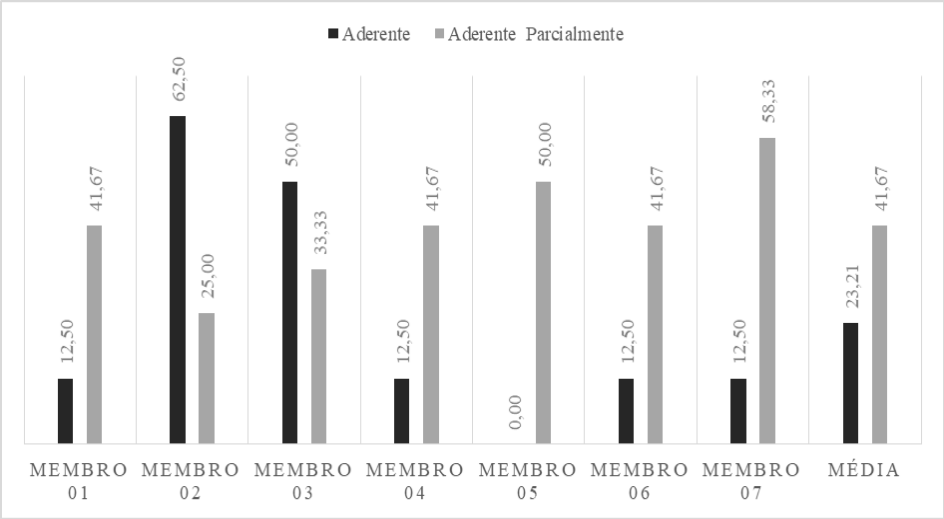


Fonte: Elaborado pelos autores.

Figura 5. Nível geral de aderência dos processos de gestão de riscos nas aquisições de TI na Prefeitura de Fortaleza - ISO 31000:2009

Conforme as informações evidenciadas na Figura 5, verifica-se que, conforme os membros participantes do Grupo Técnico de TIC, a média de aderência de todos os processos é de 14,29. Considerando o escore máximo de aderência contido na Tabela 2, que traz os quartis usados na avaliação, observa-se baixa aderência dos processos de gestão de riscos nas aquisições de tecnologia da informação na Prefeitura de Fortaleza em relação à NBR ISO 31000. Destaca-se, entretanto, que nenhum membro considerou não aderente os processos analisados. Desta forma, é possível que o Comitê que integra o Grupo Técnico de TIC da Prefeitura realize uma avaliação mais detalhada em seu processo de aquisição de ativos de TIC à luz da ISO 310000 e busque um maior grau de aderência.

Na sequência, serão apresentadas as respostas dos sete membros do Grupo Técnico de TIC da Prefeitura de Fortaleza de forma individualizada, por processo. A Figura 6 ilustra as respostas dos membros quanto ao nível de aderência do processo 5.2 - Comunicação e consulta.

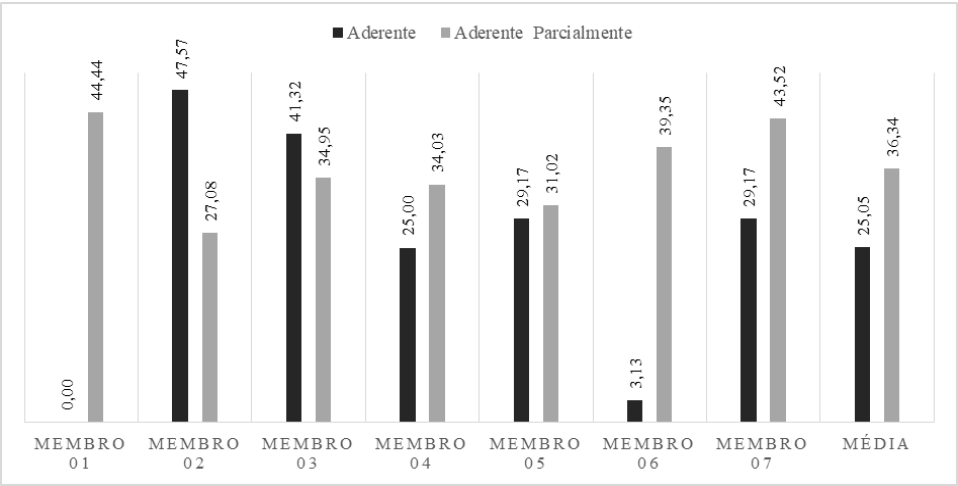


Fonte: Elaborado pelos autores.

Figura 6. Nível de aderência ao processo 5.2 - Comunicação e consulta

A partir da Figura 6, observa-se que a média de aderência do processo 5.2 - Comunicação e consulta à ISO 31000 é de 23,21%, que equivale a baixa aderência tomando como base o percentual máximo de aderência segundo a tabela de referência (Tabela 2). Destaca-se, que conforme ABNT (2009), o processo Comunicação e consulta, preconiza que 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.

A Figura 7 exibe as respostas dos membros quanto ao nível de aderência do processo 5.3 - Estabelecimento do contexto.



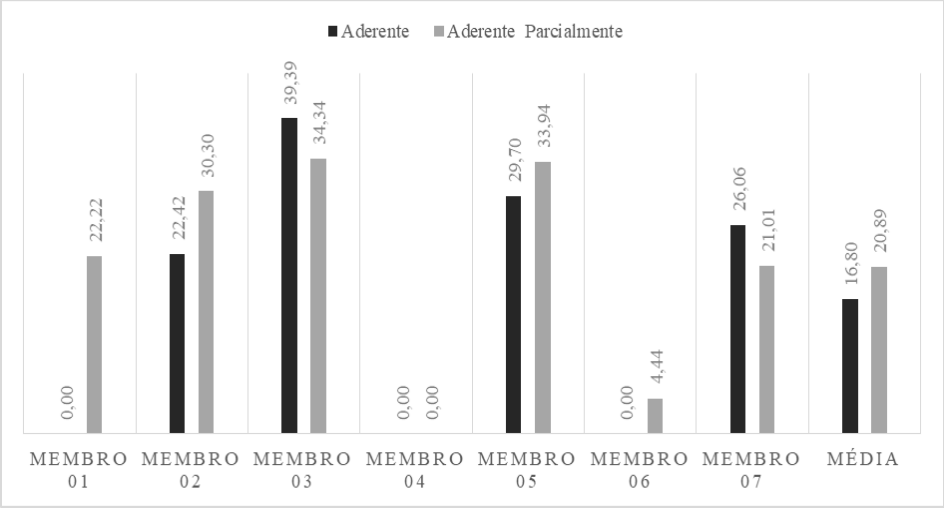
Fonte: Elaborado pelos autores.

Figura 7. Nível de aderência ao processo 5.3 - Estabelecimento do contexto

Com base na Figura 7, é possível notar que a média de aderência do processo 5.3 - Estabelecimento do contexto é de 25,05%, que equivale a média aderência tomando como base

o percentual máximo de aderência segundo a tabela de referência (Tabela 2). Conforme a ABNT (2009), o processo Estabelecimento do contexto visa que a organização realize a articulação de deus objetivos, definindo os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, estabelecendo o escopo e critérios para o restante do processo.

A Figura 8 apresenta as respostas dos membros quanto ao nível de aderência do processo 5.4 - Avaliação de riscos.

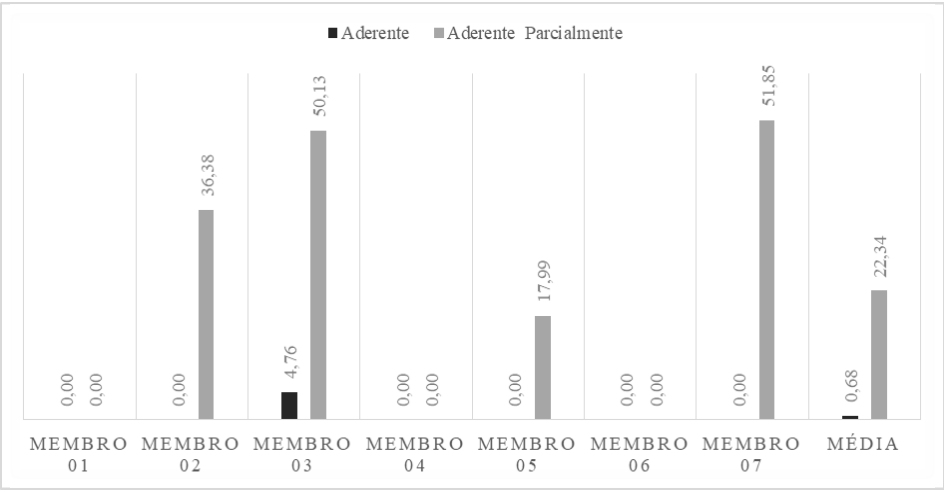


Fonte: Elaborado pelos autores.

Figura 8. Nível de aderência ao processo 5.4 - Avaliação de riscos

Verifica-se que a média de aderência do processo 5.4 - Avaliação de riscos é de 16,80%, que equivale a baixa aderência tomando como base o percentual máximo de aderência segundo a tabela de referência (Tabela 2). Em linhas gerais, conforme ABNT (2009), o processo Avaliação de riscos compreende os subprocessos de identificação, análise e avaliação de riscos.

A Figura 9 apresenta as respostas dos membros quanto ao nível de aderência do processo 5.5 - Tratamento de riscos.



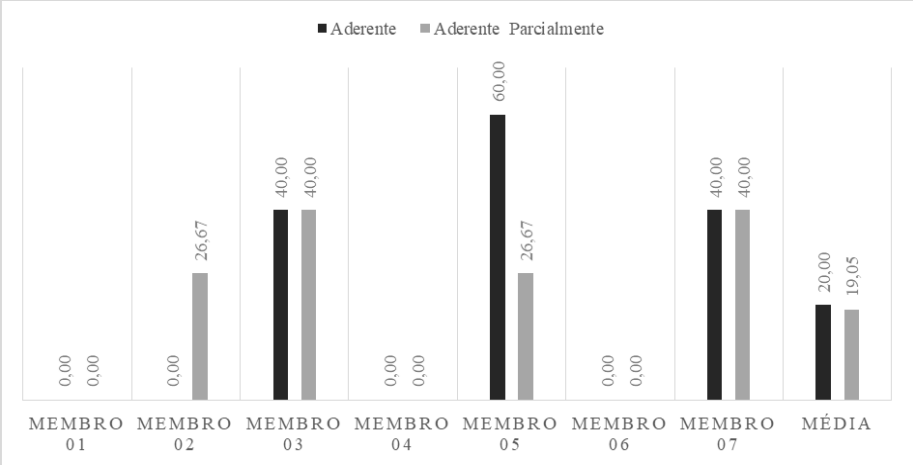
Fonte: Elaborado pelos autores.

Figura 9. Nível de aderência ao processo 5.5 - Tratamento de riscos

Com base na Figura 9, é possível notar que a média de aderência do processo 5.5 - Tratamento de riscos é de 0,68%, que equivale a baixa aderência tomando como base o

percentual máximo de aderência segundo a tabela de referência (Tabela 2). Cabe comentar que o processo Tratamento de riscos preocupa-se com a seleção e 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).

A Figura 10 exibe as respostas dos membros quanto ao nível de aderência do processo 5.6 - Monitoramento e análise crítica.

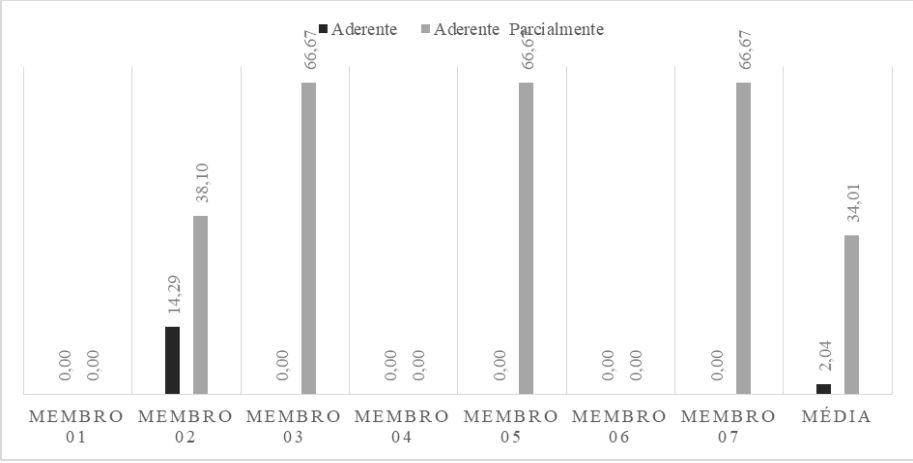


Fonte: Elaborado pelos autores.

Figura 10. Nível de aderência ao processo 5.6 - Monitoramento e análise crítica

Com base na Figura 10, é possível perceber que a média de aderência do processo 5.6 - Monitoramento e análise crítica é de 20,00%, que equivale a baixa aderência tomando como base o percentual máximo de aderência segundo a tabela de referência (Tabela 2). Segundo a ABNT (2009), o processo Monitoramento e análise crítica sinaliza que o monitoramento e a análise crítica dos riscos sejam planejados como parte da gestão e envolva a checagem e monitoramento regulares dos riscos.

A Figura 11 ilustra as respostas dos membros quanto ao nível de aderência do processo 5.7 - Registro do processo de gestão de riscos.



Fonte: Elaborado pelos autores.

Figura 11. Nível de aderência ao processo 5.7 - Registro do processo de gestão de riscos

A partir da Figura 6, observa-se que a média de aderência do processo 5.7 - Registro do processo de gestão de riscos é de 2,04%, que equivale a baixa aderência tomando como base o

percentual máximo de aderência segundo a tabela de referência (Tabela 2). Ressalta-se que o 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, ferramentas, bem como todo o processo (ABNT, 2009).

5.3 Síntese dos resultados da análise de aderência das práticas de gestão de riscos nas aquisições de TI na PMF

A Tabela 4 apresenta os processos contidos na norma ISO 31000, o percentual dos escores médios obtidos quanto à aderência das práticas de gestão de riscos nas aquisições de tecnologia da informação na PMF à luz da 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 na Prefeitura de Fortaleza à luz da ISO 31000

Processos	Percentual médio de escores obtido	Valor máximo	Nível médio de aderência
5.2 Comunicação e consulta	23,21%	24	Baixa Aderência
5.3 Estabelecimento do contexto	25,05%	85	Baixa Aderência
5.4 Avaliação de riscos	16,80%	63	Baixa Aderência
5.5 Tratamento de riscos	0,68%	54	Baixa Aderência
5.6 Monitoramento e análise crítica	20,00%	15	Baixa Aderência
5.7 Registro do processo de gestão de riscos	2,04%	21	Baixa Aderência
Total		**261**	

Fonte: Elaborado pelos autores.

A partir das informações evidenciadas na Tabela 4 é possível ter uma visão dos resultados obtidos da avaliação realizada junto ao Grupo Técnico de TIC da Prefeitura de Fortaleza, tanto de forma geral, como de forma específica para cada processo relacionado às aquisições de TI. Constata-se que há baixa aderência dos processos das práticas de gestão de riscos nas aquisições de TI considerando a ISO 31000.

É possível destacar que o processo que apresenta o maior percentual de aderência em relação à normal, com 25,05%, é o 5.3 - Estabelecimento do contexto, cujo objetivo é avaliar se durante todas as etapas ou atividades do processo de gestão de riscos, existe uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas. Assim, a PMF mostra maior atenção com este contexto, porém, precisa evoluir para o atingimento de todos os requisitos. Os menores percentuais obtidos, considerados pontos críticos para aperfeiçoamento das práticas de gestão de riscos nas aquisições de TI na Prefeitura, com 0,68% e 2,04% de aderência à ISO 31000, estão relacionados aos processos 5.5 - Tratamento de riscos e 5.7 - Registro do processo de gestão de riscos.

6 CONSIDERAÇÕES FINAIS

Considerando que a nova governança 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 ISO 31000, o nível de aderência de boas práticas de gestão de riscos nas aquisições de tecnologia da informação na Prefeitura Municipal de Fortaleza (PMF), aplicou-se um questionário estruturado para a coleta de dados primários com o mapeamento dos processos correlatos da NBR ISO 31000. Os respondentes da pesquisa corresponderam a sete dos oito gestores do

Comitê de TIC (Grupo Técnico de TIC) da PMF, sendo a aplicação do instrumento realizada entre os meses de maio e junho de 2022.

No instrumento de avaliação elaborado à luz da ISO 31000, as respostas obtidas foram balizadoras do entendimento do nível de aderência das práticas em questão e da identificação de possíveis vulnerabilidades para propor ações de boas práticas.

Em linhas gerais, os achados da pesquisa indicam importante vulnerabilidade dos processos envolvidos nas práticas de gestão de riscos nas aquisições de TI na Prefeitura de Fortaleza, quer sejam elas empíricas ou formais. Os processos e respectivos subprocessos pouco aderentes ou não aderentes à norma ISO 31000 são indicativos de revisão das práticas atualmente adotadas na Prefeitura, com destaque aos processos concernentes ao Tratamento de riscos e ao Registro do processo de gestão de riscos.

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 tecnologia da informação à ISO 31000 na Prefeitura de Fortaleza, a partir da percepção do Comitê gestor de TIC da Prefeitura. Entretanto, é pertinente ressaltar que o instrumento, à exemplo da própria norma ISO 31000, 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 profundos acerca do tema, visto que o assunto abordado é relevante para a sociedade em geral, pois todos são obrigados ao cumprimento das normas.

Por fim, tendo em vista que a presente pesquisa suscita questões ainda não resolvidas, pois é limitada à visão do gestor de tecnologia da informação (sujeitos sociais da presente pesquisa), sugere-se que futuros estudos podem considerar a percepção de analistas de segurança da informação, analistas de governança e executivos públicos. Ademais, futuras pesquisas podem analisar a adoção de boas práticas de governança sob o olhar da gestão de riscos em outras áreas das organizações públicas.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. *NBR 31000:* Gestão de riscos - Princípios e diretrizes. Rio de janeiro, 2009. Recuperado de https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf

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

Cardoso, F. F. (2019). *GRATIC:* uma metodologia para gestão de riscos em aquisições de TIC no âmbito dos institutos federais de educação. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Pernambuco, Recife, PE.

Cardoso, F. F., & Alves, C. F. (2020). GRATIC: uma metodologia para gestão de riscos em aquisições de TIC. In: *Anais do VIII Workshop de Computação Aplicada em Governo Eletrônico*. Congresso da Sociedade Brasileira de Computação (CSBC). p. 36-47.

Decreto 13.566 de 07 de abril de 2015. (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. Recuperado de https://planejamento.fortaleza.ce.gov.br/images/redes_corporativas/ti/DOM_15500_Publicao-do-Decreto-SISTIC.pdf

Santos, T. J. (2021). Gestão de riscos e a norma ISO 31000: uma abordagem literária. *Management Journal 3*(1), 1-14.

Fernandes, F. C., Kroenke, A., & Söthe, A. (2009). Uma visão atual do processo de controle e gerenciamento de riscos operacionais nos 10 maiores bancos brasileiros. In: *Anais do XII Seminários em Administração FEA/USP – SEMEAD.* São Paulo: USP.

Garcez, L. R. S. (2019). *Análise da gestão de riscos na área de compras da Fiocruz*. 111 f. Dissertação (Mestrado Profissional em Política e Gestão de Ciência, Tecnologia e Inovação em Saúde) – Fundação Oswaldo Cruz, Escola Nacional de Saúde Publica Sergio Arouca, Rio de Janeiro.

Junqueira, F. A. (2021). *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. 51 f. Dissertação (Mestrado Profissional em Administração) - Fundação Cultural Dr. Pedro Leopoldo – FPL, Pedro Leopoldo/MG.

Keller, C., & Köhler, M. (2021). Risk assessment of technology trends in supply chain management. *Journal of Supply Chain and Operations Management, 19*(2), 128.

Martin, N. C., Santos, L. R. D., & Dias Filho, J. M. (2004). Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria. *Revista Contabilidade & Finanças, 15*, 07-22.

Moraes, M. E. L. B. N. O. (2020). *Gestão de riscos no âmbito da administração pública do Distrito Federal*. 2020. 88 f. Dissertação (Mestrado Profissional em Administração Pública) – Escola de Direito e Administração Pública, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília/DF.

Netto, A. F. S. (2013). *Proposta de artefato de identificação de riscos nas contratações de TI da administração pública federal, sob a ótica da ABNT NBR ISO 31000 – Gestão de risco*s. 133 f. Dissertação (Mestrado m Engenharia Elétrica) – Universidade de Brasília - UNB, Brasília, DF.

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

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

Penha, J. C.; Parisi, C. (2005). Um caminho para integrar a gestão de riscos à controladoria. In: *Anais do XII Congresso Brasileiro de Custos*. Associação Brasileira de Custos – ABC, Florianópolis, SC, Brasil.

Pires, T. G., Cavalcante, S. M., & Corrêa, D. M. M. C. (2016). Gestão de riscos nas aquisições de soluções de TI: uma análise crítica dos modelos de boas práticas. In: *Anais do EATI - Encontro Anual de Tecnologia da Informação e STIN – Simpósio de Tecnologia da Informação da Região Noroeste do RS*. Recuperado de http://eati.info/eati/2016/assets/anais/Longos/93.pdf. Acesso em: 10 maio 2022.

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

Scannell, T., Curkovic, S., & Wagner, B. (2013). Integration of ISO 31000: 2009 and supply chain risk management. *American Journal of Industrial and Business Management, 3*(04), 367.

SEPOG - Secretaria de Planejamento Orçamento e Gestão. *Canal Planejamento e Gestão*. Recuperado de https://planejamento.fortaleza.ce.gov.br/modernizacao-administrativa/redes-corporativas/rede-de-tecnologia-da-informacao.html. Acesso em: 06 maio 2022.

Silva, D. A., Oliveira, E. C., & Canedo, E. D. (2016). Avaliação de riscos do processo de planejamento da contratação de TI: uma proposta para órgãos governamentais brasileiros. *Revista Brasileira de Sistemas de Informação, 9*(1), 168-186.

Trivelato, B. F., Mendes, D. P., & Dias, M. A. (2018). A importância do gerenciamento de riscos nas organizações contemporâneas. *Refas - Revista Fatec Zona Sul, 4*(2), 1-20.

Valentim, I. C. D., Silva, L. O., & Passos, J. G. (2016). Controle interno e gestão de risco: uma revisão baseada em estudos brasileiros. *Revista do Centro de Ciências Sociais Aplicadas, 13*(1), 69-89.

Vieira, J. B., & Barreto, R. T. D. S. (2019). *Governança, gestão de riscos e integridade*. Brasília: Enap. 240 p. Recuperado de http://repositorio.enap.gov.br/handle/1/4281. Acesso em: 06 maio 2022.