UNIVERSIDADE D
COIMBRA

Ziana Souza Santos

A GESTÃO DE RISCOS NAS INSTITUIÇÕES PÚBLICAS BRASILEIRAS: UM ESTUDO EMPÍRICO SOBRE AS SUAS PRINCIPAIS CONDICIONANTES

Dissertação no âmbito do mestrado em Gestão orientada pela Professora Doutora Patrícia Helena Ferreira Lopes Moura Sá e apresentada à Faculdade de Economia da Universidade de Coimbra

Junho de 2023

UNIVERSIDADE D
COIMBRA

Ziana Souza Santos

A GESTÃO DE RISCOS NAS INSTITUIÇÕES PÚBLICAS BRASILEIRAS: UM ESTUDO EMPÍRICO SOBRE AS SUAS PRINCIPAIS CONDICIONANTES

Dissertação no âmbito do mestrado em Gestão orientada pela Professora Doutora Patrícia Helena Ferreira Lopes Moura Sá e apresentada à Faculdade de Economia da Universidade de Coimbra para obtenção do grau de Mestre

Junho de 2023

Seja a mudança que você quer ver no mundo.

Mahatma Gandhi

AGRADECIMENTOS

Uma investigação científica demanda muita dedicação, com muitas horas de leitura, releitura, escrita e reescrita. Não é uma tarefa fácil, não é linear e demanda muita concentração, algumas noites de sono e a abdicação de alguns afazeres ou da convivência com os familiares e amigos. Apesar de exigir e depender muito do esforço pessoal do pesquisador, esta jornada não é feita sozinha, é preciso estar amparada por uma rede de apoio e de parceiros. Portanto, nada mais justo do que reconhecer e agradecer àqueles que estiveram presentes e me ajudaram em todo este percurso.

Minha enorme gratidão:

A todos os entrevistados que participaram deste estudo. A sua vontade, dedicação e entusiamo com a presente pesquisa contribuíram, sem dúvida, para a realização e a qualidade da investigação.

À Controladoria-Geral da União, que com sua política de capacitação possibilitou a concretização deste meu sonho.

À minha orientadora, Dra. Patrícia Moura e Sá, pela paciência, compreensão e notável capacidade de orientar.

Ao meu companheiro Vasco pelo apoio e por tornar mais leve a minha caminhada, e à sua família por me acolher tão bem aqui em Portugal.

Ao meu filho amado, Ilo Júnior, que sem a sua parceria neste projeto de mudar de país e de viver novos desafios nada disso seria possível.

E à Deus, pelo dom da vida e por sempre me guiar pelo caminho da luz e da sabedoria!

RESUMO

A gestão de risco tem vindo a assumir-se como uma dimensão fundamental para a excelência organizacional, em geral, e para a qualidade dos processos de governança, em particular.

No setor público brasileiro, a gestão de riscos representa um mecanismo estratégico de governança pública, de modo que a prestação de serviços e a implementação de políticas públicas alcancem os resultados pretendidos. O processo de 'institucionalização' da gestão de riscos organizacional nas entidades públicas do governo federal iniciou-se em 2016, a partir da publicação da Instrução Normativa Conjunta MP/CGU nº 01/2016 e, posteriormente, do Decreto de Governança Pública (Decreto nº 9.203, de 22 de novembro de 2017). Volvidos pouco mais de seis anos, o nível de implementação da gestão de riscos nas organizações públicas é muito variável. Algumas organizações públicas destacam-se pelo seu nível de maturidade aprimorado, mas mais de 50% das organizações não adotam ou têm sistemas incipientes.

O principal objetivo da atual pesquisa é o de mapear os fatores facilitadores e inibidores deste processo. A metodologia usada foi qualitativa com a aplicação de entrevistas semiestruturadas aos principais intervenientes no processo de implementação da gestão de riscos organizacional, selecionados com base num processo de amostragem intencional.

Os resultados revelaram que os fatores essenciais para implementar a gestão de riscos organizacional são: o sistema de governança; a política de riscos; e o apoio da alta administração. No entanto, notou-se que a existência e a consistência desses elementos dependem das características organizacionais. Em organizações onde o ambiente político é instável e a alta gestão muda constantemente (ministérios), a atuação ativa do Assessor Especial de Controle Interno (AECI) mostrou-se imprescindível para garantir o apoio da alta administração, estabelecer o modelo de governança e desenvolver a cultura de riscos.

As organizações da administração indireta, por outro lado, apresentaram um ambiente mais favorável para implementar a gestão de riscos, porque a estrutura de governança da organização já estava estabelecida e havia estabilidade dos seus dirigentes.

O sistema de TIC não se mostrou essencial para iniciar a implementação da gestão de riscos, mas, à medida que a organização avançava em seus processos mapeados ou nas etapas de monitoramento e comunicação dos riscos, a ferramenta mostrou-se fundamental.

Independentemente do ambiente organizacional, os entrevistados destacaram que a atuação da auditoria interna governamental (Audin e CGU) contribuiu substancialmente para o desenvolvimento da cultura de riscos da organização. Além disso, notou-se uma expectativa maior em relação à CGU em prestar os serviços de consultoria e avaliação dos processos de gestão de riscos da organização.

Esses resultados têm implicações práticas e teóricas. Primeiro, o extenso mapeamento realizado pela presente pesquisa pode contribuir de alguma maneira para identificar boas práticas na implementação de sistemas de gestão de riscos e servir de referência para as organizações que desejam implantar ou melhorar o seu processo de gestão de riscos organizacional. Segundo, apresenta subsídios para atuação da auditoria interna governamental na melhoria do processo de implementação da gestão de riscos das organizações públicas. Do lado teórico, este estudo contribui com evidências empíricas dos direcionadores essenciais para se implementar a gestão de riscos em organizações do setor público brasileira e inova em apresentar resultados empíricos de casos múltiplos no contexto da administração pública.

Palavras-chave: Gestão de riscos. Setor público. Governança Pública. Auditoria Interna. CGU.

ABSTRACT

Risk management has become a fundamental dimension for organizational excellence, in general, and for the quality of governance processes, in particular.

In the Brazilian public sector, risk management represents a strategic public governance mechanism, so that the provision of services and the implementation of public policies achieve the intended results. The process of 'institutionalization' of organizational risk management in public entities of the federal government began in 2016, from the publication of the Normative Instruction MP/CGU nº 01/2016 and, later, of the Public Governance Decree (Decree nº 9,203, of November 22, 2017). A little over six years later, the level of implementation of risk management in public organizations is very variable. Some public organizations stand out for their improved maturity level, but more than 50% of organizations do not adopt or have incipient systems.

The main objective of the current research is to map the facilitating and inhibiting factors of this process. The methodology used was qualitative with the application of semi-structured interviews to the main players in the process of implementing organizational risk management, selected based on an intentional sample process.

The results revealed that the essential factors to implement enterprise risk management are: the governance system; the risk policy; and support from top management. However, it was noted that the existence and consistency of these elements depend on organizational characteristics. In organizations where the political environment is unstable and top management is constantly changing (ministries), the active role of the Special Advisor for Internal Control (AECI) proved to be essential to guarantee the support of top management, establish the governance model and develop the risk culture.

Indirect administration organizations, on the other hand, presented a more favorable environment to implement risk management, because the organization's governance structure was already established and there was stability in its directors.

The IT system did not prove to be essential to start implementing risk management, but as the organization advanced in its mapped processes or in the risk monitoring and communication stages, the tool proved to be fundamental.

Regardless of the organizational environment, the interviewees highlighted that the performance of the governmental internal audit (Audin and CGU) contributed substantially to the development of the organization's risk culture. In addition, there was a greater expectation in relation to the CGU in providing consultancy services and evaluation of the organization's risk management processes.

These results have practical and theoretical implications. First, the extensive mapping carried out by this research can contribute in some way to identifying good practices in the implementation of risk management systems and serve as a reference for organizations that wish to implement or improve their organizational risk management process. Second, it presents subsidies for the performance of the governmental internal audit in the improvement of the risk management implementation process of public organizations. On the theoretical side, this study contributes with empirical evidence of the essential drivers to implement risk management in Brazilian public sector organizations and innovates by presenting empirical results of multiple cases in the context of public administration.

Keywords: Risk management. Public sector. Public Governance. Internal Audit. CGU.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

AECI ..... *Assessoria Especial de Controle Interno*

AGR ..... *Agentes de Riscos*

Audin ..... *Auditorias Internas Singulares*

CGRC ..... *Comitê de Governança, Riscos e Controle*

CGU ..... *Controladoria-Geral da União*

COSO ..... *Committee of Sponsoring Organizations of the Treadway Commission*

ERM ..... *Enterprise Risk Management*

IGG ..... *Índice Geral de Governança do Setor Público*

IIA ..... *Institute of Internal Auditors*

ISO ..... *International Organization for Standardization*

OCDE ..... *Organização para a Cooperação e Desenvolvimento Econômico*

PGR ..... *Política de Gestão de Riscos*

SCI ..... *Sistema de Controle Interno*

TCU ..... *Tribunal de Contas da União*

TIC ..... *Tecnologia da Informação e Comunicação*

UAIG ..... *Unidades de Auditoria Interna Governamental*

INDÍCE

1. INTRODUÇÃO

A ineficiência do gasto público do Brasil consome uma parcela relevante do seu Produto Interno Bruto (PIB). Segundo relatório do Banco Interamericano de Desenvolvimento (BID), publicado em 2019, que analisa o gasto público no Caribe e América Latina, a ineficiência alocativa e técnica do gasto público no Brasil, relacionada a fatores como falta de profissionalismo, negligência, corrupção, ou uma combinação deles, é da ordem de 3,9% do PIB ao ano (BID, 2018; OECD, 2020).

A busca pela boa governança pública é uma necessidade eminente para melhorar a qualidade da gestão pública, assegurar maior responsividade (accountability), transparência e integridade (integrity) das organizações públicas (BRASIL, 2018a; Vieira & Barreto, 2019). Como mecanismo de governança, a gestão de riscos é crucial para reduzir a possibilidade de resultados adversos na implementação de políticas públicas, programas, projetos e na prestação de serviços públicos. Enquanto as organizações do setor privado adotam a gestão de riscos para sustentar a lucratividade, as organizações públicas usam a gestão de riscos para garantir uma prestação de serviço ininterrupta contra riscos internos e externos e para manter a responsabilidade pública (Mahama, Elbashir, Sutton, & Arnold, 2022).

Diferentemente do contexto internacional, a iniciativa de implementar a gestão de riscos no setor público brasileiro é relativamente recente. As primeiras iniciativas da gestão de riscos corporativos no governo federal tiveram início na década de 1990, mas somente a partir da publicação da Instrução Normativa Conjunta MP/CGU nº 1, de 2016, da Lei nº 13.303, de 2016 e do Decreto nº 9.203, de 2017, a prática passou a ser largamente difundida (OECD, 2012; Souza, Braga, Cunha, & Sales, 2020; Vieira & Barreto, 2019).

As normas recentes do setor público brasileiro indicam o desejo contínuo do governo de modernizar seu sistema atual orientado à conformidade, introduzindo uma abordagem de tomada de decisão mais estratégica que reconhece claramente a necessidade do fortalecimento da gestão de riscos como mecanismo da boa governança pública. Contudo, a realidade mostra que, para dar efetividade aos princípios e práticas da boa governança pública, as reformas legais embora sejam necessárias para a institucionalização, não são suficientes para garantir uma implementação efetiva das

medidas (Vieira & Barreto, 2019). A experiência de países membros da OCDE e de organizações da administração pública federal indireta com experiência em gestão de riscos sugerem que pode levar de três a cinco anos para estabelecer as bases para uma cultura positiva de gestão de riscos (OECD, 2012).

Após seis anos da 'institucionalização' da gestão de riscos organizacional nas entidades públicas do governo federal, nota-se que o nível de implementação da gestão de riscos nas organizações públicas é muito variável. Em que pese a sua relevância, boa parte das organizações públicas do governo federal ainda não tem o seu processo de gestão de riscos implantado ou ainda é incipiente, segundo levantamento realizado pelo Tribunal de Contas da União em 2021 (BRASIL, 2021).

Nesse contexto, o propósito desta pesquisa é estudar quais os direcionadores para a implementação de uma gestão de riscos bem-sucedida nas organizações públicas. Para tanto, adotou-se uma abordagem qualitativa descritiva-exploratória. Para coletar os dados empíricos, o método escolhido foi a aplicação de entrevista semiestruturadas aos principais intervenientes no processo de implementação da gestão de riscos organizacional, selecionados com base num processo de amostragem intencional.

Na revisão de literatura efetuada não se identificou pesquisa exploratória de estudos de casos múltiplos, com o fim de avaliar os principais direcionadores para a implementação da gestão de riscos no setor público brasileiro. Portanto, além de contribuir para a literatura científica sobre gestão de riscos no setor público, espera-se que o resultado da atual pesquisa contribua para identificar boas práticas na implementação de sistemas de gestão de riscos; sirva de referência para as organizações que desejam implantar ou melhorar o seu processo de gestão de riscos organizacional; e contribua com informações relevantes para subsidiar as estratégias de atuação das unidades de auditoria interna governamental no processo de gestão de riscos das organizações públicas.

A presente dissertação está estruturada em 4 grandes capítulos. O primeiro é o referencial teórico que traz importantes conceitos que serão utilizados no decorrer do estudo e faz a revisão de literatura de suporte ao tema da pesquisa. O segundo explica em detalhe a metodologia aplicada. O terceiro apresenta os resultados encontrados e faz a discussão sobre os achados. Por fim, a conclusão com os principais achados, as contribuições do estudo, as limitações encontradas e propostas de estudos futuros.

2. CAPÍTULO I - REFERENCIAL TEÓRICO

2.1. Conceitos

2.1.1. Governança

O termo governança surgiu no setor privado no final do século XX e representou um momento de transformação dos modelos de gestão das empresas. As novas formas de propriedade demandaram novos mecanismos e estruturas empresariais para garantir formas de controle por parte dos proprietários/acionistas sobre as decisões e o desempenho das empresas, assim como para reduzir os conflitos entre sócios majoritários e minoritários (BRASIL, 2020b).

No âmbito das organizações públicas, a proliferação de sentidos e usos do termo governança, entre acadêmicos e gestores, surgiu a partir de 1980 e está associada a pelo menos três aspectos centrais. Primeiro, a baixa utilização do termo governança até os anos 1970 é indicativa de que a solução para os problemas de desempenho e de responsabilização do setor público até então tinha uma resposta única: o modelo de administração burocrático tradicional. Segundo, a expansão da utilização do termo governança na virada do século aparece associada à difusão de pacotes de reforma do aparato estatal internacionalmente difundidos e abrigados sob o movimento da nova gestão pública (new public management – NPM). E o terceiro aspecto, mais contemporâneo, refere-se à crescente percepção da complexificação dos problemas, das possibilidades de solução e dos sentidos de desempenho e responsabilização no setor público (Cavalcante & Pires, 2018).

No Brasil, o tema governança pública ascendeu à agenda do Executivo federal a partir das contribuições do Tribunal de Contas da União (TCU) e da Controladoria-Geral da União (CGU), órgãos do controle externo e do controle interno, respectivamente. Os órgãos de controle protagonizaram a discussão sobre governança, prescrevendo medidas consideradas promotoras da chamada “boa” governança para órgãos da administração direta e indireta (Nogueira & Gaetani, 2018).

A primeira publicação específica sobre governança pública foi o Referencial Básico de Governança do TCU[1], de 2013, aplicável a órgãos e entidades da administração pública. Desde então, diversos normativos institucionalizaram a aplicação de mecanismos e práticas da boa governança pública, a exemplo da Lei das Estatais (Lei nº 13.303/2016), que estabeleceu regras de governança corporativa, de transparência, práticas de gestão de riscos e de controle interno para as empresas públicas, sociedades de economia mista e suas subsidiárias; da Instrução Normativa Conjunta MP/CGU nº 1, de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal; e do Decreto nº 9.203/2017, que instituiu a política de governança da administração pública federal (BRASIL, 2020b; Souza et al., 2020; Vieira & Barreto, 2019).

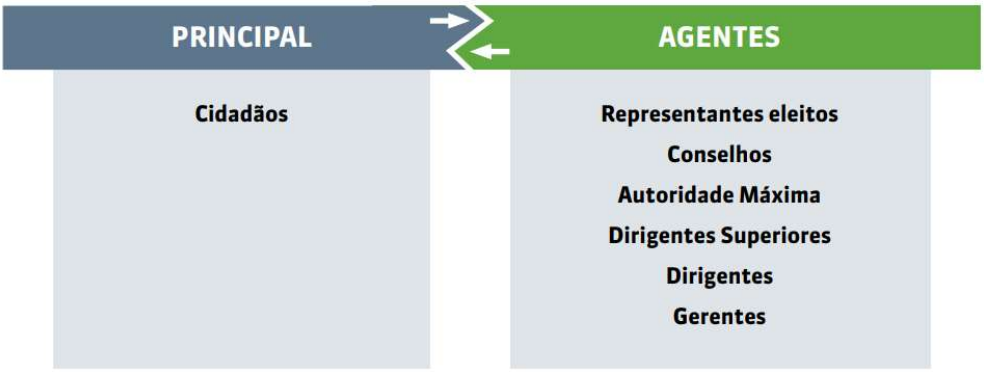
As normas recentes do setor público brasileiro indicam o desejo contínuo do governo de modernizar seu sistema atual orientado à conformidade, introduzindo uma abordagem de tomada de decisão mais estratégica que reconhece claramente a necessidade do fortalecimento da gestão de riscos como mecanismo da boa governança pública. A teoria da agência apoia essa visão de que o estabelecimento de um sistema de controle interno eficaz alinha as ações e decisões da gestão de acordo com os melhores interesses das partes interessadas e proporciona um ambiente favorável para a avaliação e monitoramento dos controles internos e riscos da organização (Abidin, 2017).

Assim como a governança corporativa, a governança pública organizacional parte do mesmo problema: o conflito agente-principal. No âmbito da administração pública brasileira, o povo (o cidadão) é o principal[2]. Por outro lado, todas as pessoas que, em seu papel institucional, implementam a estrutura do Estado brasileiro são os "agentes", ou agentes públicos, que estão necessariamente a serviço do povo (BRASIL, 2020b).

Figura 1 - Relação principal-agente no setor público

[1] O Referencial Básico de Governança do TCU encontra-se disponível para download em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/

[2] Constituição Federal de 1988, art. 1º: "Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição"

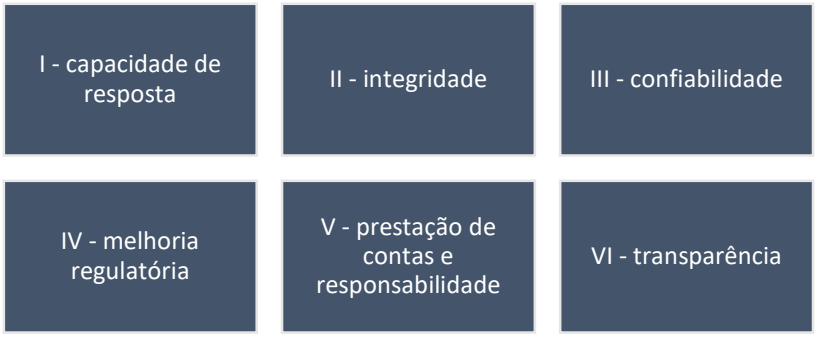


Fonte: (BRASIL, 2020b, p. 38)

Para entregar o valor público[3] à sociedade, os princípios sobre os quais se desenvolve a boa governança pública, aplicáveis a qualquer tipo de organização, independentemente de porte, natureza jurídica ou tipo de controle, devem ser sempre observados.

Esses princípios da governança pública funcionam como valores interdependentes, servindo de guia para a atuação das organizações públicas na busca dos resultados pretendidos e fortalecendo a confiança da sociedade nessas organizações (BRASIL, 2020b):

Figura 2- Listas de princípios da governança pública



Fonte: Decreto 9.203/2017, art. 3º.

Enquanto a governança é responsável por estabelecer a direção a ser tomada, a gestão é a função responsável por planejar a forma mais adequada de implementar

[3] Art. 2º do Decreto 9.203/2017: valor público - produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos.

as diretrizes estabelecidas, executar os planos e fazer o controle de indicadores e de riscos (BRASIL, 2020b).

Figura 3 - Relação entre governança e Gestão

Fonte: (BRASIL, 2020b, p. 38)

Uma governança bem estabelecida permite aos mandatários de uma organização pública avaliar sua situação e demandas, direcionar a sua atuação e monitorar o seu funcionamento, de modo a aumentar as chances de entrega de bons resultados aos cidadãos, em termos de serviços e de políticas públicas (BRASIL, 2020b, p. 15).

2.1.2. Controle Interno

O controle interno é um processo desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos da organização (COSO, 2013). Esse processo envolve um conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, devendo ser conduzidos de forma integrada pela estrutura de governança, pelos gestores e pelo corpo funcional das organizações (BRASIL, 2016; COSO, 2013).

A Instrução Normativa Conjunta MP/CGU nº 1, de 2016, que dispõe sobre controles internos no âmbito do Poder Executivo federal, especifica os objetivos gerais a serem alcançados pelas organizações públicas:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;
b) cumprimento das obrigações de accountability;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos.

Dada a sua função, os controles internos não devem ser implementados de forma circunstancial, devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, a complexidade, a estrutura, a missão e os objetivos da organização (BRASIL, 2016, 2017a). Esses controles internos constituem-se na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos (BRASIL, 2017a).

É importante não confundir os controles internos da gestão com as atividades do Sistema de Controle Interno (SCI) do Poder Executivo federal, nem com as atribuições da auditoria interna governamental, cuja finalidade específica é a medição e avaliação da eficácia e eficiência dos controles internos da gestão (BRASIL, 2016).

O Sistema de Controle Interno compreende as atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização. Atualmente, o SCI do Poder Executivo federal tem como órgão central a Controladoria-Geral da União (CGU), criada pela Lei nº 10.683, de 28 de maio de 2003 (BRASIL, 2016).

2.1.3. Auditoria Interna Governamental

A auditoria interna é uma atividade independente e objetiva de avaliação (*assurance*) e consultoria, criada para agregar valor e melhorar as operações de uma organização (BRASIL, 2016, 2017a; IIA, 2020). A atividade de auditoria interna governamental constitui a terceira linha das organizações e tem como objetivo auxiliar a organização a atingir seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada à avaliação e melhoria da eficácia dos processos de gestão de riscos, controles internos, integridade e governança (BRASIL, 2016, 2017a; BRASIL & Controladoria Geral da União, 2017).

A atividade de auditoria interna governamental no Poder Executivo federal é exercida pelo conjunto de Unidades de Auditoria Interna Governamental (UAIG) elencadas

a seguir: a) Secretaria Federal de Controle Interno (SFC) e as Controladorias Regionais da União nos estados, que fazem parte da estrutura da Controladoria-Geral da União (CGU); b) Secretarias de Controle Interno (Ciset) da Presidência da República, da Advocacia-Geral da União, do Ministério das Relações Exteriores e do Ministério da Defesa, e respectivas unidades setoriais; c) auditorias internas singulares (Audin) dos órgãos e entidades da administração pública federal direta e indireta; e d) o Departamento Nacional de Auditoria do Sistema Único de Saúde (Denasus) do Ministério da Saúde (BRASIL, 2017a).

Compete à CGU, como órgão central do SCI, e aos órgãos setoriais nas respectivas áreas de jurisdição prover orientação normativa e supervisão técnica às UAIG. A orientação normativa e a supervisão técnica são exercidas mediante a edição de normas e orientações técnicas e a avaliação da atuação das UAIG, com o objetivo de harmonizar a atividade de auditoria interna governamental, promover a qualidade dos trabalhos e integrar o Sistema (BRASIL, 2017a).

O trabalho de avaliação, como parte das atividades de auditoria interna, pode ser definido como a obtenção e a análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria (CGU, 2017). Na atividade de avaliação da adequação dos processos de gestão de riscos, a auditoria interna deve verificar se os riscos significativos são identificados e avaliados; se as respostas aos riscos são estabelecidas de forma compatível com o apetite a risco da organização; e se as informações sobre riscos relevantes são coletadas e comunicadas de forma oportuna (CGU, 2017; IIA, 2017).

Já o serviço de consultoria consiste em assessoramento, aconselhamento, treinamento, facilitação, dentre serviços relacionados fornecidos à alta administração com a finalidade de respaldar as operações da unidade (CGU, 2017). Muito embora a gestão dos riscos seja uma responsabilidade fundamental da gestão organizacional, os auditores internos que atuam numa função de consultoria podem ajudar a organização a identificar, avaliar e implementar metodologias e controles de gestão de risco para fazer face a esses riscos(CGU, 2017; IIA, 2017).

Avaliar os processos de gestão de riscos da organização é diferente da exigência de que os auditores utilizem a análise de risco para planejar auditorias (IIA, 2017). O planejamento da atividade de auditoria deve considerar as estratégias, os objetivos, as

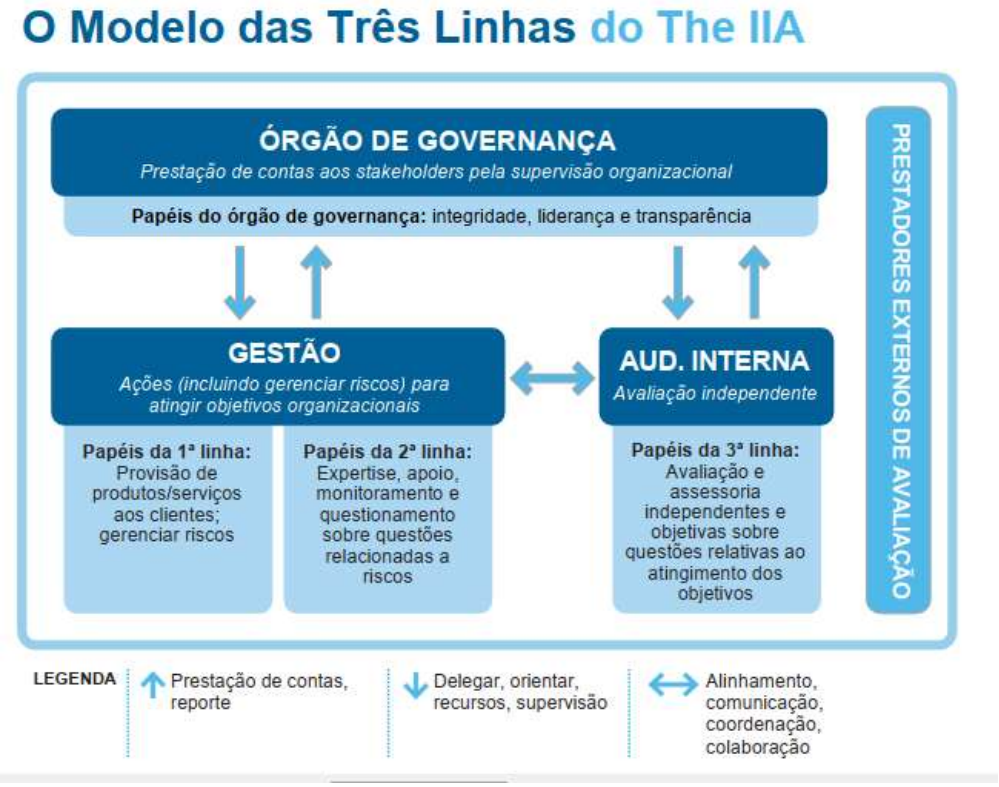
prioridades, as metas da organização e os riscos a que seus processos estão sujeitos (BRASIL, 2017a). A abordagem da auditoria baseada em riscos tem como principal finalidade garantir que a unidade de auditoria interna governamental concentre seus trabalhos nos objetos de auditoria com maior exposição a riscos que possam afetar o alcance dos seus objetivos(CGU, 2017).

A auditoria interna governamental, embora apresente muitas semelhanças com a auditoria independente, apresenta suas especificidades. Entre elas, pode-se destacar: a) a obtenção e a análise de evidências relativas à utilização dos recursos públicos, a qual contribui diretamente para a garantia da *accountability* nas suas três dimensões, quais sejam: transparência, responsabilização e prestação de contas; b) a contribuição para a melhoria dos serviços públicos, por meio da avaliação da execução dos programas de governo e da aferição do desempenho dos órgãos e das entidades no seu papel precípuo de atender à sociedade; c) a atuação com vistas à proteção do patrimônio público (CGU, 2017).

2.1.3.1. Modelo das Três Linhas

O Modelo das Três Linhas, proposto pelo Instituto dos Auditores Internos (*Institute of Internal Auditors [IIA]*), visa assegurar que a informação proveniente do processo de gestão de riscos seja adequadamente comunicada e utilizada como base para a tomada de decisões e para a responsabilização em todos os níveis organizacionais, sendo aplicável a qualquer organização, ainda que não exista uma estrutura ou sistema formal de gestão de riscos (BRASIL, 2018a; IBGC, 2017)

Figura 4 - O modelo das três linhas do IIA



Fonte: (IIA, 2020)

A governança de gestão de riscos pressupõe a existência de interação entre todos os níveis da organização, incluindo os diversos órgãos de governança e de apoio à governança, bem como os agentes da primeira, segunda e terceira linhas (IBGC, 2017). O Modelo é mais eficaz quando adaptado para se alinhar aos objetivos e circunstâncias da organização (IIA, 2020).

O órgão de governança determina a direção da organização, definindo a visão, missão, valores e apetite organizacional a riscos. Em seguida, delega a responsabilidade pelo atingimento dos objetivos da organização à gestão, juntamente com os recursos necessários. O órgão de governança pode estabelecer comitês para prestar supervisão adicional sobre aspectos de sua responsabilidade, como auditoria, riscos, finanças, planejamento e remuneração (IIA, 2020).

A gestão operacional e os procedimentos rotineiros de riscos e controles internos constituem a primeira linha na gestão de riscos. Na primeira linha ocorre a gestão do risco por meio das atividades cotidianas dos gestores de identificar, avaliar, gerir e comunicar os riscos. Nesse nível ocorre a implementação de políticas e procedimentos internos que

oferecem garantia razoável de que as atividades estão de acordo com as metas e os objetivos (BRASIL, 2018a; Vieira & Barreto, 2019).

A segunda linha é constituída por funções – unidades, comitês ou outras estruturas organizacionais – estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão de riscos e controles (BRASIL, 2018a). Na segunda linha as funções específicas podem variar entre organizações, mas normalmente os papéis incluem monitoramento, assessoria, orientação, teste, análise e reporte sobre assuntos relacionados à gestão de riscos. É comum que os líderes da segunda linha, como o chefe da área de riscos, tenham uma linha de reporte direto ao órgão de governança (IBGC, 2017; IIA, 2020).

No âmbito da administração pública do Poder Executivo federal, os Assessores e Assessorias Especiais de Controle Interno (AECI) nos ministérios integram a segunda linha e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações (BRASIL, 2017a).

A terceira linha é representada pela atividade de auditoria interna governamental, que presta serviços de avaliação (*assurance*) e de consultoria com base nos pressupostos de autonomia técnica e de objetividade (BRASIL, 2017a). O papel fundamental da auditoria interna na gestão de riscos é fornecer uma garantia aos órgãos de governança e à alta administração de que os processos de gestão de riscos operam de maneira eficaz e os maiores riscos do negócio são gerenciados adequadamente em todos os níveis (Vieira & Barreto, 2019).

O modelo de três linhas de defesa é relevante porque comunica claramente os papéis e as responsabilidades na estruturação da governança. O órgão de governança, a gestão e a auditoria interna têm responsabilidades distintas, mas todas as atividades precisam estar alinhadas com os objetivos da organização. Além disso, são necessárias colaboração e comunicação entre os papéis de primeira e segunda linha da gestão e auditoria interna, a fim de garantir que não haja duplicação, sobreposição ou lacunas desnecessárias. A base para uma coerência bem-sucedida é a coordenação, colaboração e comunicação regulares e eficazes (IIA, 2020).

2.1.4. Gestão de Riscos

O risco é usado para expressar incerteza sobre eventos ou quando seus resultados podem ter um efeito material sobre os objetivos da organização (Selim, 1999). Quando a incerteza se torna gerenciável, ela passa a ser considerada um risco (Power, 2007). Em outras palavras, o risco envolve a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos pelas organizações. Sendo o risco inerente a qualquer atividade – e impossível de eliminar –, a sua administração é um elemento-chave para a sobrevivência de todo e qualquer tipo de organização (IBGC, 2017; ISO, 2018).

A gestão de riscos pode ser entendida como um processo estruturado e iterativo, de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, para gerir e controlar os riscos a que a organização está sujeita, destinado a fornecer segurança razoável quanto à realização de seus objetivos (COSO, 2017; ISO, 2018).

A gestão de riscos contribui para uma mudança de foco de conformidade para o de responsabilidade que enfatiza a medição de desempenho e a formulação de estratégias (Rana, Hoque, & Jacobs, 2019). Isso porque a definição de uma estratégia demanda um processo decisório estruturado que analisa os riscos e alinha os recursos com a missão e a visão e valores fundamentais da organização (COSO, 2017).

A implementação de um processo formal de gestão de risco (ERM) por uma organização ajuda a obter uma visão geral dos diferentes riscos (e interdependências de risco) a que estão expostas, reduz o tempo de reação a questões relacionadas com o risco, cria uma cultura positiva de risco, e melhora o processo de mitigação de riscos (Castanheira, Rodrigues, & Craig, 2010).

No longo prazo, a gestão de riscos corporativos pode também aumentar a resiliência da organização – a capacidade de se antecipar e responder a mudanças. Isso porque ela ajuda as organizações a identificar fatores que representam mudanças, e como essas mudanças podem afetar o desempenho e demandar revisão da estratégia (COSO, 2017).

Dentre os principais modelos internacionais de gestão de riscos, destacam-se: a) o modelo proposto pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) para Gestão de Riscos Corporativos (Enterprise Risk Management

[ERM]), conhecido como modelo “COSO ERM” ou COSO II; e b) o modelo da Organização Internacional de Normalização (*International Organization for Standardization* [ISO]), conhecido como Norma ISO 31000.

2.2. Modelos Internacionais de Gestão de Riscos Corporativos

2.2.1. COSO – ERM 2004

O Committee of Sponsoring Organizations of the Treadway Commission (COSO) é uma iniciativa do setor privado, patrocinado e financiado pelas principais associações de classe de profissionais da área financeira e contábil dos Estados Unidos da América (EUA)[4]. Desde a sua criação em 1985, o COSO procurou promover práticas relacionadas ao controle interno. Em 1992, o COSO publicou a obra Internal Control - integrated framework (COSO-IC ou COSO I), com o objetivo de ajudar as organizações a avaliar e aperfeiçoar seus sistemas de controle interno de modo a assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes.

A partir de 2001 nos EUA eclodiram uma série de escândalos financeiros e quebras de negócios de grande repercussão (Enron, Parmalat, Worldcom, etc), que geraram grandes prejuízos a investidores, empregados e outras partes interessadas. Na esteira desses eventos, vieram solicitações de melhoria dos processos de governança corporativa e gerenciamento de riscos, por meio de novas leis, regulamentos e de padrões a serem seguidos. Nesse contexto, em 2004, o COSO publicou o Enterprise Risk Management - integrated framework (COSO-ERM ou COSO II), com o propósito de fornecer estratégia de fácil utilização pelas organizações para avaliar e melhorar a gestão de riscos (COSO, 2004; Dias, 2017).

O COSO ERM (ou COSO II) não teve o objetivo de substituir a estrutura de controles internos das organizações (COSO I), porém trouxe incorporada a estrutura de controle interno em seu conteúdo, o que permite às empresas tanto atender às suas necessidades de controle interno, quanto adotar um processo completo de gerenciamento de riscos

[4] O COSO é formado por representantes da American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives Internationl (FEI), Institute of Managements Accountants (IMA) e pelo Institute of Internal Auditors (IIA)

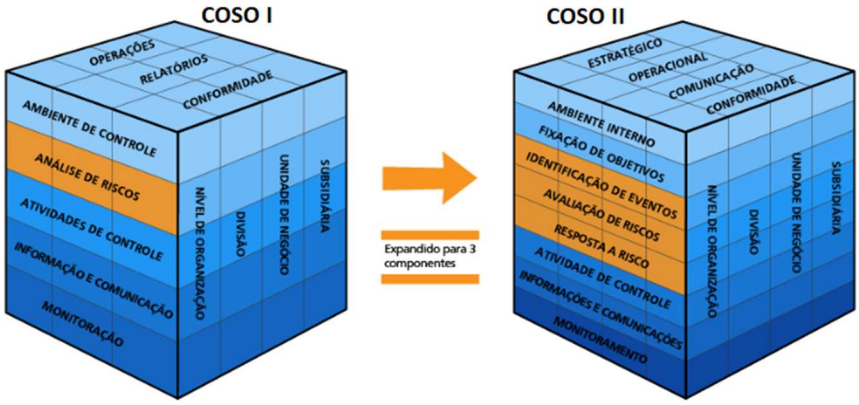
(COSO, 2004). Igualmente ao COSO I, o modelo de gerenciamento de riscos é também apresentado na forma de matriz tridimensional (cubo), demonstrando uma visão integrada dos componentes para gerenciar os riscos, no contexto dos objetivos e da estrutura de cada organização.

Figura 5 - COSO ERM - Matriz tridimensional - Objetivos, Componentes e Estruturas

Fonte: COSO ERM - adaptada

Com maior enfoque em risco, o modelo amplia o componente de gerenciamento de riscos da estrutura de controle interno, criando quatro componentes: fixação de objetivos (que é um pré-requisito do controle interno), identificação de eventos, avaliação de riscos e resposta a riscos (COSO, 2004). A figura a seguir mostra como o COSO I faz parte do COSO II e como o sistema de controle interno pode ser visto como parte integrante do sistema de gerenciamento de riscos:

Figura 6- COSO I (ou COSO-IC) e COSO II (ou COSO ERM) adaptado para o português



Fonte: imagem extraída do portal do TCU

Enquanto o COSO I se concentra mais nos riscos operacionais e seus controles, o COSO II, a partir da nova categoria de objetivos “Estratégico”, considera cada vez mais os riscos estratégicos. Segundo o modelo, os objetivos estratégicos fluem da missão ou da visão da organização, enquanto os objetivos operacionais, de comunicação e de conformidade devem estar alinhados a eles. O gerenciamento de riscos corporativos é aplicado para se definir a estratégia, assim como as ações para que esses objetivos sejam alcançados nas outras três categorias.

Ainda referente às categorias de objetivos, a “Comunicação” na estrutura do COSO I relaciona-se com a confiabilidade das demonstrações financeiras publicadas, enquanto em COSO ERM, a categoria de comunicação foi expandida significativamente, a fim de envolver todos os relatórios desenvolvidos pela organização, divulgados tanto interna quanto externamente. Seu alcance não se limita a cobrir as informações financeiras em um caráter mais amplo, mas inclui também as informações não financeiras.

O COSO-ERM introduz, ainda, os conceitos de apetite a riscos e a tolerância a risco. O apetite a riscos é a quantidade de risco estabelecida, de modo amplo que uma empresa está disposta a aceitar na busca de sua missão/visão. Ele serve como ponto de referência para se fixar as estratégias e a escolha dos objetivos correlatos. Por outro lado, as tolerâncias a riscos são os níveis aceitáveis de variação referentes à realização dos objetivos.

2.2.2. Novo COSO – ERM (COSO 2017)

Publicado em 2017, a nova versão, agora intitulada Enterprise Risk Management – Integrating with Strategy and Performance (Gerenciamento dos Riscos Corporativos – Integrado com Estratégia e Performance) ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance.

Para (Dias, 2017) este novo COSO ERM parece ser bastante diferente do anterior, considera o autor que sua atualização é uma reação às críticas e sugestões feitas por especialistas ao longo dos anos.

Por outro lado, (Prewett & Terry, 2018) observam que houve pouca novidade no COSO ERM de 2017, tendo o seu foco na definição de estratégia e desempenho e no

reconhecimento mais profundo do papel da governança e da cultura. Para os autores, o que é mais importante no novo COSO ERM é a ênfase nos dois primeiros princípios, “Governança e Cultura” e “Estratégia e Definição de Objetivos”. Esses dois princípios promovem o conceito de ERM que permeia a organização, elevando a responsabilidade da gestão de riscos corporativos aos mais altos níveis de gestão e criando uma cultura em toda a empresa incorporada e informada pelo ERM.

Em um nível conceitual, o Instituto Brasileiro de Governança Corporativa (IBGC) propõe os seguintes níveis de maturidade em relação ao estágio de gestão de riscos corporativos de uma organização: i) inicial, ii) fragmentado, iii) definido, iv) consolidado e v) otimizado. No âmbito das organizações públicas, o Tribunal de Contas da União (TCU) propôs os cinco níveis de maturidade: i) inicial, ii) básico, iii) intermediário, iv) aprimorado e v) avançado. Para o nível mais baixo de maturidade “inicial”, a prática de gestão de riscos é realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização. Ou seja, o risco é gerenciado ad hoc ou separadamente em “silos”. À medida que a organização consegue estabelecer as funções da 2ª linha (ou chief risk officer [CRO]), adotar uma abordagem de “portfólio” ou “holística” para o risco, estabelecer indicadores chaves de riscos consistentes e monitorá-los periodicamente, o seu nível de maturidade avança. O nível máximo de maturidade é alcançado quando a cultura de riscos e controles é efetiva em todos os níveis da organização, os processos de gestão de riscos estão bem integrados aos objetivos estratégicos, as tecnologias integradas habilitam a gerenciar os riscos em toda organização, e há o uso de uma abordagem padronizada e consistente para definir o apetite e tolerância a riscos (BRASIL, 2021; IBGC, 2017).

Para (Farrell & Gallagher, 2015) o mais alto nível de maturidade organizacional da gestão de riscos ocorre quando as discussões baseadas em riscos estão inseridas em um nível estratégico, como planejamento de longo prazo, alocação de capital e tomada de decisão. Assim como, quando o apetite e as tolerâncias de risco são claramente compreendidos com alertas para garantir que as instâncias de governança e a gerência executiva sejam informadas quando os limites de risco forem excedidos. Para (Prewett & Terry, 2018) a intenção do COSO ERM 2017 parece ser ajudar a mover as empresas para este mais alto nível de maturidade, o qual está associado a um maior valor da empresa.

As organizações que integraram com sucesso o processo de gestão de riscos em suas atividades estratégicas e práticas cotidianas, resultante da governança e cultura, exibem capacidade superior em descobrir dependências e correlações de risco em toda a organização e, como consequência, agregar valor (Farrell & Gallagher, 2015). Nesse sentido, a ênfase nos dois primeiros princípios, “Governança e Cultura” e “Estratégia e Definição de Objetivos” parece ser o que há de mais importante no modelo, e ser a principal contribuição do COSO ERM 2017 (Prewett & Terry, 2018).

Para a definição da estratégia, o COSO 2017 ressalta a importância de se considerar o risco nesta fase porque as causas mais importantes de destruição de valor residem na possibilidade de a estratégia não suportar a missão e a visão da entidade, e nas implicações decorrentes da estratégia escolhida (COSO, 2017).

Assim, a gestão de riscos corporativos envolve tanto entender as implicações da estratégia escolhida e a possibilidade de seu eventual desalinhamento, como gerenciar os riscos associados aos objetivos de negócios. A definição de uma estratégia demanda um processo decisório estruturado que analise os riscos e alinhe os recursos com a missão e a visão e valores fundamentais da organização. A figura a seguir ilustra essas considerações no contexto da missão, visão e valores fundamentais, e como determinantes dos direcionadores estratégicos e da performance da entidade (COSO, 2017).

Figura 7- COSO ERM 2017 - Relacionamento da estratégia no contexto da missão, visão e valores, e como determinantes da performance da entidade

Fonte: Sumário Executivo COSO 2017

Uma vez que o risco influencia e alinha estratégia e desempenho em toda organização, o COSO 2017 realça a importância da gestão de riscos corporativos no planejamento estratégico e a sua incorporação em toda a organização (COSO, 2017).

Para tanto, os cinco componentes do novo COSO se combinam em um conjunto de 20 (vinte) princípios que abrangem desde a governança até o monitoramento. Eles descrevem práticas que podem ser aplicadas de diferentes formas nas organizações, independentemente do seu tamanho, tipo ou setor econômico. A adoção dos princípios pode trazer às instâncias de governança a segurança de que a organização é capaz de gerenciar em um nível aceitável os riscos associados à estratégia e aos objetivos de negócios (COSO, 2017).

Figura 8- COSO ERM 2017 – Componente e Princípios

Fonte: Sumário Executivo COSO 2017 – adaptada

Para (Prewett & Terry, 2018), ao contrário do cubo ERM simplista de 2004, o ícone principal do novo COSO é esotérico e abstrato. Os cinco componentes parecem ser versões reformuladas dos cinco componentes de controle interno do COSO, e a maioria dos conceitos contidos nos 20 princípios descritos no ERM de 2017 estão incluídos no ERM de 2004, embora não com tantos detalhes.

Figura 9 - Comparação entre COSO ERM 2017 e COSO ERM 2004

2017 Component	#	2017 Principle	Included in 2004 Model?	2004 Component
Governance & Culture	1	Exercises Board Risk Oversight	✓	Internal Environment
	2	Establishes Operating Structures	✓	
	3	Defines Desired Culture	✓	
	4	Demonstrates Commitment to Core Values	✓	
	5	Attracts, Develops, and Retains Capable Individuals	✓	
Strategy & Objective-Setting	6	Analyzes Business Context	✓	Objective Setting
	7	Defines Risk Appetite	✓	
	8	Evaluates Alternative Strategies	ø	
	9	Formulates Business Objectives	≠	
Performance	10	Identifies Risk	✓	Event Identification
	11	Assesses Severity of Risk	≠	Risk Assessment
	12	Prioritizes Risk	✓	
	13	Implements Risk Responses	✓	Risk Response & Control Activities
	14	Develops Portfolio View	✓	Risk Response
Review & Revision	15	Assesses Substantial Change	✓	Monitoring
	16	Reviews Risk and Performance	✓	
	17	Pursues Improvement in Enterprise Risk Management	✓	
Information, Communication & Reporting	18	Leverages Information Technology	✓	Information & Communication
	19	Communicates Risk Information	✓	
	20	Reports on Risk, Culture, and Performance	✓	

Legend: ✓ Topic is included
≠ Some key concepts are missing
ø Most key concepts are missing

Fonte: (Prewett & Terry, 2018)

2.2.3. ISO 31000:2018

A ISO 31000 foi publicada inicialmente em 2009 (ISO 31000:2009), mas atualmente está na versão 2018 (31000:2018). É uma norma internacional da família de gestão de risco criada pela International Organization for Standardization (ISO). Ela é composta por três normas: ISO 31000 – Informações básicas, princípios e diretrizes para a implementação da gestão de riscos; ISO/IEC 31010 – Técnicas para avaliação de riscos; e 31073 – Vocabulário relacionado à gestão de riscos.

A ISO 31000:2018 Gestão de Riscos – Diretrizes, diferentemente do COSO ERM, não tem abordagem prescritiva, trazendo em seu texto princípios e diretrizes gerais sobre a gestão de riscos. Os princípios, a estrutura e o processo de gestão de riscos da ISO 31000 são baseados no padrão australiano e neozelandês AS/NZS 4360. (Hutchins, 2018)

As definições da ISO 31000:2018 são amplas e discricionárias, abertas à interpretação, para que possam ser usadas em diferentes aplicações, funções, setores e contextos. Isso foi amplamente intencional pela ISO ((Hutchins, 2018). Pela sua simplicidade e por ser mais fácil de implementar, muitas empresas preferem usar a ISO 31000 para Gestão de Riscos (Dias, 2017).

Contudo, se por um lado, a natureza descritiva da norma é uma grande vantagem, por outro lado representa também ser sua fraqueza. Isso porque as definições mais críticas podem perder sua especificidade e se tornar discricionárias ou, na pior das hipóteses, arbitrárias. Assim, para evitar este resultado, (Hutchins, 2018) argumenta que a norma carece da devida orientação de um profissional de risco.

Atualmente a ISO 31000:2018 está presente em mais de 60 países como padrão nacional de risco. Adequadamente arquitetada, projetada e implementada, a ISO 31000 pode oferecer muitos benefícios, como, por exemplo (Hutchins, 2018):

Quadro 1 - Lista de benefícios da ISO 31000:2018

- Incentivar a tomada de decisão proativa e preventiva, em vez do gerenciamento reativo
- Identificar e tratar os riscos em toda a empresa
- Melhorar a identificação de oportunidades e ameaças
- Cumprir os requisitos legais e regulamentares
- Melhorar os relatórios financeiros
- Melhorar a governança corporativa, risco e conformidade (GRC)
- Melhorar a confiança das partes interessadas
-Estabelecer uma base confiável para tomada de decisão e resolução de problemas baseada em risco

Fonte: (Hutchins, 2018)

2.2.4. COSO ERM 2017 vs ISO 31000:2018

O COSO ERM 2017 e a ISO 31000:2018 são padrões que estabelecem as melhores práticas para identificar, avaliar e responder a riscos. Embora ambas as estruturas se preocupem com o gestão de riscos, existem algumas diferenças importantes entre elas, como, por exemplo, a existência de orientações sobre como desenvolver um programa de gerenciamento de riscos corporativos (ERM), previsto somente no COSO ERM 2017. Para (Hutchins, 2018), o Framework 2017 pode ser referenciado como "ERM pesado" porque é mais abrangente e a gestão de riscos corporativa tem ênfase na governança. Já a ISO 31000:2018 tem um foco tático e de processo e, portanto, é referenciada como ERM de nível básico ou "ERM leve".

Além disso, o COSO 2017 foi projetado para ser integrado aos processos de negócios existentes de uma organização, enquanto a ISO 31000 pode ser implementada como um sistema de gestão de riscos independente.

Quadro 2 - Comparação entre COSO ERM 2017 e ISO 31000:2018

CATEGORIAS	COSO ERM 2017	ISO 31000:2018
Escopo	Diferentes formas de organizações, independentemente do seu tamanho, tipo ou setor econômico.	Qualquer tipo de organização, contexto, atividade ou setor.
Características	É uma norma prescritiva.	É uma norma descritiva.
Riscos	É a possibilidade de que os eventos ocorram e afetem a realização da estratégia e dos objetivos de negócios.	É o efeito da incerteza nos objetivos.
	Os eventos podem gerar impacto tanto negativo quanto positivo ou ambos.	O efeito pode ser tanto negativo quanto positivo ou ambos.
Apetite a risco (COSO) **Critério de risco (ISO)**	Os tipos e a quantidade de risco, em um nível amplo, que uma organização está disposta a aceitar em busca de valor.	É a quantidade e tipo de risco que a organização pode ou não assumir em relação aos objetivos estratégicos

CATEGORIAS	COSO ERM 2017	ISO 31000:2018
Gestão de riscos corporativos (COSO) **Gestão de riscos (ISO)**	ERM é a cultura, as competências e as práticas que as organizações integram à definição e à execução da estratégia, com o objetivo de gerenciar o risco na criação, na preservação e na realização de valor.	são atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.
Avaliação de riscos[1]	Os riscos identificados são avaliados para entender a gravidade[2] de cada um para o alcance da estratégia e dos objetivos de negócios da entidade. A avaliação permite que a gestão priorize os riscos e aloque recursos para que o risco se mantenha dentro do apetite a risco da organização.	Envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional.
Estrutura (COSO)/ Processo (ISO) da Gestão de Riscos	Composta de 5 componentes, combinados com seus 20 princípios: 1. Governança e Cultura; 2. Estratégia e Definição de Objetivos; 3. Desempenho; 4. Análise e Revisão; Informação, comunicação e relatórios	É um processo iterativo e compreende em seis etapas: 1. Comunicação e consulta; 2. Escopo, contexto e critérios; 3. Processo de avaliação de riscos; 4. Tratamento de riscos; e 5. Monitoramento e análise crítica; e 6. Registro e relato

Fonte: elaboração prória

[1] Na ISO 31000:2018 há também a definição para o processo de avaliação de riscos que compreende de três etapas: identificação, análise e avaliação de riscos.

[2] COSO ERM 2017 estabelece que a gravidade é medida considerada como a probabilidade e o impacto dos eventos ou o tempo que leva para se recuperar dos eventos.

2.3. Gestão de Riscos na Administração Pública brasileira

A iniciativa de implantar a gestão de riscos no setor público é relativamente recente no Brasil, embora, em alguns países, tenha começado há mais tempo. No Reino

Unido, no início dos anos 1990, foi implantada com a finalidade de aumentar o empreendedorismo no setor público e, desde então, vem se consolidando como parte integrante do processo de gestão pública em muitos países (BRASIL, 2018a).

As organizações públicas atuam em ambientes nos quais fatores como instabilidade política-administrativa, restrições orçamentárias, recursos tecnológicos e humanos limitados, permanentes mudanças regulatórias e normativas, execução de políticas públicas descentralizadas, dentre outros fatores, geram incertezas. A incerteza emana da incapacidade de se determinar com precisão a probabilidade de ocorrência de determinados eventos e impactos a eles associados(COSO, 2004).

A capacidade de tomar decisões corretas em ambiente caracterizado por incertezas, é fundamental. A boa gestão dos riscos é crucial para reduzir a possibilidade de resultados adversos na implementação de políticas públicas, programas, projetos e na prestação de serviços públicos.

No contexto brasileiro, as primeiras iniciativas, ainda na década de 1990, aconteceram de modo fragmentado em algumas organizações do governo federal, a exemplo dos bancos comerciais públicos que iniciaram a gestão de riscos operacionais fortemente influenciados pelas obrigações internacionais do Comitê de Supervisão Bancária da Basiléia (OECD, 2012). O quadro a seguir traz exemplos de algumas dessas organizações.

Quadro 3 – Exemplos das primeiras iniciativas de gestão de riscos nas organizações públicas brasileiras

Organização	Histórico das primeiras iniciativas de gestão de riscos
Banco do Brasil (BB)	A gestão do risco operacional tornou-se preocupação no final da década de 90, quando o sistema de controles internos foi oficialmente implantado pela Presidência Executiva. Em 2002, criou o Comitê de Riscos Operacionais e, no ano seguinte, criou diretoria específica para o gerenciamento dos riscos de mercado, de crédito e operacional. (Trapp & Corrar, 2005)
Banco Central do Brasil (BCB)	Iniciou em 1997 a formalização de técnicas de gestão de riscos de mercado para a gestão das reservas internacionais. Em 2000, desenvolveu a abordagem de gestão de riscos financeiros para administração desses ativos e, em 2006, criou uma política e uma estrutura para a gestão de

	riscos financeiros envolvendo unidades operacionais na área de política monetária. Em 2011, formalizou a Política de Gestão de Riscos (PGR) para toda a Instituição, englobando tanto os riscos financeiros como os riscos não financeiros. (Manual de Gestão Integrada de Riscos)
Secretaria do Tesouro Nacional (STN)	Iniciou em 2003 a implementação de projeto-piloto na Secretaria-Adjunta responsável pela administração da dívida pública para desenvolvimento e implantação de metodologia de gerenciamento de riscos operacionais na STN. (Relatório de Gestão da STN de 2005)
Receita Federal do Brasil (RFB)	As práticas de gestão de riscos estratégicos já aconteciam de modo nem sempre sistematizado. A partir de 2010 com a criação da Coordenação de Gestão de Riscos – Coris e a adoção de metodologia específica (qualitativa e quantitativa), a cultura de gestão de riscos estava, pouco a pouco, sendo disseminada e implementada internamente. (Relatório de Gestão da RFB de 2010)
Agência Nacional de Saúde Suplementar (ANS)	A ANS iniciou seu projeto de estruturação e implementação da Gestão de Riscos desde 2013, com a criação da Coordenadoria de Avaliação de Risco Institucional (COARI), seguida de importantes avanços em 2014, com a publicação da sua Política de Gestão de Riscos - Resolução Administrativa nº 60, de 15 de julho de 2014. (Relatório de Gestão da ANS de 2015)

Fonte: elaboração própria

Nota-se, no entanto, que até então só havia iniciativas pontuais e limitadas entre as organizações da administração pública direta e indireta para a implementação da gestão de risco operacional.

No âmbito da CGU, o cenário começou a mudar a partir de 2012, quando a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) fez a primeira avaliação do sistema de integridade da administração pública federal brasileira, com importantes recomendações no intuito de melhorar a governança pública e a gestão dos riscos que afetam as operações e o desempenho das organizações públicas. O relatório destacou a importância da integração da gestão de riscos como um elemento central da responsabilidade da gestão, a fim de promover a integridade e prevenir má conduta, desperdício e corrupção (OECD, 2012; Souza et al., 2020).

Dentre as recomendações feitas, destacam-se: “i) avançar na implementação da gestão de riscos nas organizações públicas federais; ii) monitorar o impacto e eficácia da auditoria interna; e iii) fortalecer a coordenação entre as autoridades do governo central para integrar a gestão de riscos em futuras reformas de gestão (OECD, 2012, p. 173).

Em seu relatório a OCDE apontou lacunas na gestão de riscos e destacou o papel central da CGU no apoio e indução da implementação de sistemas de gestão de riscos nos órgãos da administração pública federal (Souza et al., 2020). Além disso, ressaltou o desafio do controle interno brasileiro em conduzir as reformas referentes ao fortalecimento do controle interno como uma série separada das reformas gerenciais da administração pública. Isso porque a experiência dos países membros da OCDE na implementação da gestão de riscos exigiu a responsabilidade final da gestão do controle interno. Assim, dada a segregação de atribuições entre a CGU e o então Ministério do Planejamento, Orçamento e Gestão (MP), a introdução da gestão de riscos e o fortalecimento do controle interno teriam que ser conduzidos em conjunto com as reformas gerenciais de forma mais geral, a fim de posicionar a administração como responsável pela manutenção de um sistema sólido de controle interno (OECD, 2012).

Em 2016, impulsionados pela avaliação da OCDE, o então Ministério do Planejamento (MP) e a Controladoria-Geral da União (CGU) publicaram a Instrução Normativa Conjunta MP/CGU nº 1, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal(Souza et al., 2020). Em 2017, foi publicado o Decreto da Política de Governança da administração pública federal – Decreto nº 9.203, de 2017, e também apresentada a proposta de Projeto de Lei nº 9.163, de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

A partir da publicação da Instrução Normativa nº 1/2016, a CGU, no âmbito das suas atribuições de auditoria interna governamental, passou a ter as competências de: “I – avaliar a política de gestão de riscos dos órgãos e entidades do Poder Executivo federal; II – avaliar se os procedimentos de gestão de riscos estão de acordo com a política de gestão de riscos; e III – avaliar a eficácia dos controles internos da gestão implementados pelos órgãos e entidades para mitigar os riscos, bem como outras respostas aos riscos avaliados”. Ainda em 2016, por meio do Decreto nº 8.910, de 22 de novembro de 2016, a CGU passou

a ter a atribuição de, nas atividades de auditoria e fiscalização, propor melhorias e aprimoramentos na gestão de riscos dos órgãos e entidades da administração pública federal. Em 2019, por meio do Decreto nº 9.681, de 3 de janeiro de 2019, a CGU incorporou a atribuição de promover capacitação e orientação técnica sobre a gestão de riscos nos órgãos e nas entidades da administração pública federal.

Paralelo a essas mudanças, o Tribunal de Contas da União também desenvolveu diversas iniciativas com o objetivo de fomentar a gestão de riscos na administração pública federal. A partir de 2012, começou a mapear a situação da gestão de riscos de entidades da administração indireta, e, posteriormente, já em 2017, extendeu esta avaliação também para todas as entidades do setor público, no âmbito do Índice Geral de Governança do Setor Público (IGG) (BRASIL, 2020a). Além disso, o TCU desevolveu diversos manuais sobre gestão de riscos, os quais encontram-se disponíveis no seu portal na Internet para download : i) Referencial de combate a fraude e corrupção (2017 e 2018); ii) Referencial básico de gestão de riscos (2018); iii) Roteiro de avaliação de maturidade em gestão de riscos (2018); iv); 10 passos para a boa gestão de riscos (2018); e v) Manual de Gestão de Riscos do TCU (2017 e 2020).

2.3.1. Modelo de Gestão de Riscos do Governo Federal

A Instrução Normativa Conjunta MP/CGU nº 1/2016, que estabelece que os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança, está dividida em três grandes temas essencialmente correlacionados. Primeiro, o controle interno da gestão que deve ter por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pela organização. Segundo, a gestão de riscos que permite o estabelecimento de procedimentos de controles internos proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização. E terceiro, a governança pública, que, para garantir que as ações das organizações públicas estejam alinhadas com o interesse público, considera essencial a gestão de riscos e os controles internos como mecanismos de estratégia e

controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão (BRASIL, 2016, 2017b).

Figura 10 - Relação entre Governança, Gestão de Riscos e Controles Internos

Fonte: (BRASIL, 2018a)

A nova norma enfatiza a importância de integrar a gestão de riscos e controle interno de forma que o ambiente de controle e gestão de riscos respeite os valores, interesses e expectativas da organização e de todas as partes interessadas, tendo o cidadão e a sociedade como principais vetores.

Como estrutura de governança interna da unidade, a IN define que o dirigente máximo da organização deverá instituir o Comitê de Governança, Riscos e Controle (CGRC), composto pela autoridade máxima e pelos demais dirigentes a ele subordinados diretamente. O CGRC deverá ser apoiado pelo respectivo Assessor Especial de Controle Interno.

Considerando a composição do CGRC e as respectivas competências estabelecidas no §2º do art. 23 da IN, nota-se que este comitê tem por objetivo final envolver a alta administração e engajar os dirigentes nos mecanismos e práticas de governança pública. Isso porque a governança e a cultura de gestão de riscos são a base dos demais componentes de gestão de riscos na organização. A governança define o tom (*tone at the top*), reforça a importância e estabele as responsabilidades pela gestão de riscos. A cultura de riscos deve permear toda a organização, e cabe à alta administração engajar-se para

promover um amplo entendimento da importância do tema para a melhoria da tomada de decisão e alcance dos objetivos organizacionais (IBGC, 2017).

No capítulo referente à gestão de riscos, observa-se que a Instrução Normativa Conjunta MP/CGU nº 1/2016 baseou-se nos modelos COSO ERM 2004 e ISO 31000:2009 (Souza et al., 2020). Muito embora a norma prescreva requisitos e parâmetros mínimos a serem seguidos pelas organizações, ela permite aos órgãos e entidades certa autonomia para a customização de seus modelos de gestão de riscos de acordo com a sua estrutura de governança, cultura e recursos disponíveis, especialmente quanto ao estabelecimento da política de gestão de riscos e da metodologia e ferramentas a serem empregadas pela organização. As principais características da norma estão apresentadas no quadro a seguir:

Quadro 4 – Características do modelo da Gestão de Riscos estabelecido na Instrução Normativa Conjunta MP/CGU nº 1/2016

TÓPICOS	DESCRIÇÃO
Escopo	Órgãos e entidades do Poder Executivo federal.
Definições:	
➢ **Apetite a risco**	Nível de risco que uma organização está disposta a aceitar.
➢ **Riscos**	Possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;
➢ **Gerenciamento de riscos**	Processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização.
➢ **Política de gestão de riscos**	Declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.
Estrutura da Política de Gestão de Riscos	A política de gestão de riscos a ser instituída pelos órgãos e entidades públicas, no prazo de até doze meses, a partir da vigência da IN, deve conter, pelo menos, a seguinte estrutura: I – princípios e objetivos organizacionais; II – diretrizes sobre a integração da gestão de riscos ao planejamento estratégico, aos processos e às políticas da organização; o processo de identificação, avaliação, monitoramento e comunicação dos riscos; a estrutura de governança interna da gestão de riscos; e metodologias e ferramentas; III – e a matriz de responsabilidades para a efetivação da gestão de riscos.
Estrutura do modelo de Gestão de Riscos[1]	Na implementação e atualização do modelo de gestão de riscos deverá observar os seguintes componentes da estrutura de gestão de riscos:

TÓPICOS	DESCRIÇÃO
	I – ambiente interno; II– fixação de objetivos; III – identificação de eventos; IV – avaliação de riscos; V – resposta a riscos; VI – atividades de controles internos; VII – informação e comunicação; e VIII – monitoramento.
Tipologias de riscos	Ao efetuar o mapeamento e avaliação dos riscos, deve considerar, entre outras possíveis, as seguintes tipologias de riscos: a) riscos operacionais; b) riscos de imagem/reputação do órgão; c) riscos legais; e d) riscos financeiros/orçamentários
Matriz de responsabilidades	- Cabe ao dirigente máximo estabelecer a estratégia e a estrutura da gestão de riscos da organização; - Compete à alta administração avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada; - Os gestores são os responsáveis pela avaliação dos riscos que lhe são afetos; - Cada risco mapeado e avaliado deve ter um agente responsável formalmente identificado
Modelo de Governança	Os órgãos e entidades do Poder Executivo federal deverão instituir, pelos seus dirigentes máximos, Comitê de Governança, Riscos e Controles, o qual deverá ser composto pelo dirigente máximo e pelos dirigentes das unidades a ele diretamente subordinadas e será apoiado pelo respectivo Assessor Especial de Controle Interno.
Competências do CGRC	- Ao Comitê de Governança, Riscos e Controles, no âmbito da gestão de riscos, compete: i) institucionalizar estruturas adequadas de gestão de riscos; ii) incentivar a adoção de boas práticas de gestão de riscos; iii) aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos; iv) supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público; v) estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública, ou atividade; vi) aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos; vii) emitir e monitorar recomendação para o aprimoramento da gestão de riscos.

Fonte: Elaboração própria a partir da IN º1, de 2016

[1] Mesmos componentes do modelo COSO ERM 2004 para gerenciar riscos

2.3.2. Nível de Maturidade em gestão de riscos das organizações públicas

Em 2017, o Tribunal de Contas da União (TCU) criou o Índice Geral de Governança do Setor Público (iGG) para avaliar a governança pública da administração pública federal brasileira (BRASIL, 2021).

Em 2018, por meio do Acórdão 588/2018[5] - Plenário, o TCU deliberou pela continuidade da avaliação, por um período de cinco anos, a fim de: identificar riscos sistêmicos; subsidiar o Tribunal e o Congresso Nacional com informações de qualidade sobre a governança e a gestão das organizações públicas; orientar sua atuação na seleção de unidades a serem auditadas; contribuir para o aperfeiçoamento da governança e da gestão públicas e acompanhar o desenvolvimento institucional brasileiro.

Desta forma, este levantamento passou a ocorrer anualmente, à exceção de 2020 que, em decorrência da pandemia, não aconteceu e foi adiado para 2021.

O método utilizado para a obtenção do Perfil Integrado de Governança Organizacional e Gestão Públicas foi o CSA (*Control Self-Assessment* - autoavaliação de controles), preconizado pelo IIA (*The Institute of Internal Auditors*). O questionário de autoavaliação eletrônico e padronizado em 2021 foi aplicado ao conjunto de 381 unidades jurisdicionadas do TCU, a fim de obter informações acerca da maturidade da governança e da capacidade de gestão dessas organizações.

A estrutura do questionário do iGG2021[6] dispôs de 36 práticas avaliadas por meio de 114 itens de verificação, e foi respondido de forma válida por 378 organizações. As questões foram agrupadas pelos temas: Governança pública; Gestão de pessoas; Gestão de tecnologia e da segurança da informação; Gestão de contratações; e Gestão orçamentária.

[5] Link para o Acórdão: TCU ACÓRDÃO 588/2018 – PLENÁRIO

[6] https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/

Os resultados do levantamento das 378 organizações basearam nos dados declarados pelos respondentes e no método de classificação (estágios de capacidade) apresentado na figura abaixo:

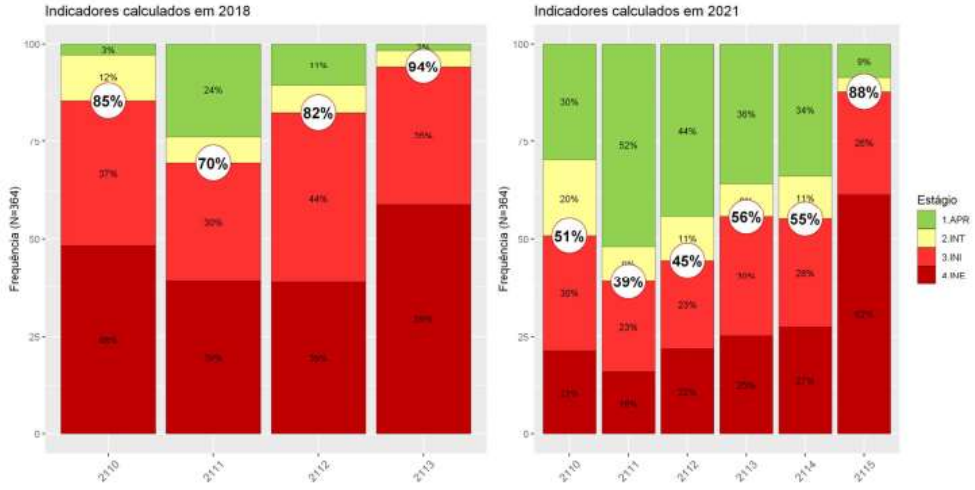
Figura 11 - Categorização de respostas e limites de estágios de capacidade

Fonte: Perfil Integrado de Governança Organizacional e Gestão Públicas – 2021, TCU

Para avaliar a prática "Gerir riscos (2110)", considerou-se as seguintes questões ou itens de verificação: 2111. A estrutura da gestão de riscos está definida; 2112. Atividades típicas de segunda linha estão estabelecidas; 2113. O processo de gestão de riscos da organização está implantado; 2114. Os riscos considerados críticos para a organização são geridos; e 2115. A organização executa processo de gestão de continuidade do negócio.

Segundo levantamento, conforme figura a seguir, houve sensível melhora na prática "gerir riscos", comparativamente ao panorama identificado em 2018 (85% e 51% no estágio inicial, em 2018 e 2021 respectivamente), mesmo considerando o conjunto maior de itens de controle utilizados para avaliar essa prática no questionário aplicado em 2021.

Figura 12 - Gerir Riscos: comparativo entre 2018 e 2021



Fonte: Perfil Integrado de Governança Organizacional e Gestão Públicas – 2021, TCU

Na análise do TCU, esta evolução pode ter sido resultado dos novos requisitos normativos e esforços orientativos no tema, a exemplo do Decreto 9.203/2017 e da Lei das Estatais (Lei 13.303/2016), que abordam diversos aspectos da prática de gestão de riscos a serem observados pelas organizações públicas da administração federal direta e indireta; assim como os manuais publicados no repositório de conhecimento da Controladoria-Geral da União (CGU) sobre gestão de riscos e integridade.

Em que pese o progresso, ainda há muito o que melhorar, uma vez que mais da metade (51%) das organizações respondentes ainda declaram "não adotar" ou "adotar em menor parte" (coluna 2110) prática amplamente aceita e difundida na literatura acerca da governança, e já normatizada no Brasil (BRASIL, 2021).

2.4. Os direcionadores para a implementação de uma gestão de riscos bem-sucedida

Vários pesquisadores têm procurado entender as variáveis que impulsionam a implementação de um sistema de gestão de risco (Bracci, Mouhcine, Rana, & Wickramasinghe, 2022; Mahama et al., 2022; Rana, Wickramasinghe, & Bracci, 2019; Woods, 2009). A abordagem da teoria da contingência diz que, embora as estruturas básicas da gestão de riscos sejam comuns em grandes organizações, podem surgir contingências específicas que mobilizarão outras interdependências (Woods, 2009).

Assim, assume-se a premissa de que não existe um sistema de gestão de riscos universalmente apropriado que se aplique a todas as organizações e em todas as circunstâncias. Esta seção resume os direcionadores para a implementação da gestão de riscos, encontrados nos artigos pesquisados, e que serviram de referências para o presente estudo exploratório.

(Mahama et al., 2022) propuseram uma estrutura para a gestão de riscos corporativo/organizacional (ERM) com três elementos necessários para que as organizações desenvolvam processos eficazes de ERM operando dentro e fora dos limites organizacionais. O primeiro é o desenvolvimento de estratégias de gerenciamento de riscos que se alinham com a missão, os objetivos organizacionais e toda a cadeia de valor.

O segundo elemento são atividades de governança apropriadas onde o envolvimento dos funcionários em diferentes níveis é incentivado e mecanismos para alocar responsabilidade e supervisão são estabelecidos (Mahama et al., 2022). Avaliando as reformas promovidas pelo governo australiano em 2013, (Barrett AO, 2014) destacou que para a gestão de riscos desempenhar um papel significativo na melhoria do desempenho das organizações públicas, o envolvimento ministerial (e a prestação de contas) é essencial, assim como, a comunicação estreita e o envolvimento real de todas as partes interessadas. Em outras palavras, as estruturas de governança e gestão são essenciais para implementar uma gestão de riscos real e eficaz.

Em terceiro lugar, o ERM prospera no ideal de ferramentas de TIC para apoiar o processo de gestão de riscos, estabelecer os limites de risco, monitar, medir, comunicar e corrigir(Mahama et al., 2022). Na mesma linha, (Woods, 2009) defente que o sistema de gerenciamento de risco depende diretamente das ferramentas de TIC porque essa tecnologia é parte integrante do processo de controle de risco e vital para a prestação de serviços. Por exemplo, uma avaliação de desempenho abrangente exige que cada diretoria monitore seus riscos e que a alta administração também tenha acesso a informações atualizadas sobre os níveis atuais de exposição a riscos de toda organização (Woods, 2009).

Em seu estudo de caso, para além da variável de TIC, (Woods, 2009) especifica que o ERM depende de mais outras duas variáveis também principais: a política do governo central; e o tamanho organizacional. Das variáveis de contigências ela sugere que a política do governo central sobre os sistemas de controles internos e gestão de riscos é a mais poderosa das variáveis, porque influencia implicitamente o nível de investimento das organizações nesses sistemas. Em relação ao tamanho, dentro das organizações maiores há uma tendência para sistemas de controle formalizados/padronizados, com presença de equipe de especialistas de riscos e de representantes de risco nomeados por cada diretoria para implementar uma "abordagem prática e viável para a gestão de risco dentro de sua diretoria".

(Selim & McNamee, 1999b) apontam que nas organizações que estavam na vanguarda do desenvolvimento e implementação dos processos de gestão de riscos a auditoria interna conseguiu tornar-se um parceiro no domínio da gestão de riscos. Isto ocorreu porque a auditoria interna: 1. participou da determinação e compreensão do risco

estratégico; 2. estabeleceu ligações importantes entre os processos estratégicos e os riscos e entre os processos operacionais e os riscos; 3. desenvolveu a comunicação necessária entre planos estratégicos e planos de auditoria; 4. adotou a mudança de paradigma da auditoria baseada em controles para a auditoria baseada no risco.

A Comissão de Auditoria do Reino Unido também reconheceu que a auditoria interna tem um papel vital a desempenhar na revisão dos processos de gerenciamento de riscos estabelecidos e, mais fundamentalmente, em fornecer garantia aos dirigentes e gestores sobre a eficácia dos controles (Audit Commission, 2001).

(Abidin, 2017) destaca a necessidade de um acompanhamento eficaz da extensão da exposição aos riscos inerentes à estratégia organizacional por meio da função de auditoria interna e dos programas de auditoria baseados no risco. A auditoria interna baseada no risco ajuda as empresas a praticar uma gestão eficaz dos riscos, uma vez que incorpora princípios de gestão de risco durante todo o processo de auditoria, tanto no processo de planejamento anual, como no planejamento de cada trabalho de auditoria (Castanheira et al., 2010).

3. CAPÍTULO II - METODOLOGIA

3.1. Estratégia e questões de pesquisa

Para (Yin, 2010), o estudo de caso adequa-se a questões de pesquisa sobre o 'como' e o 'porquê', quando o investigador tem pouco controle sobre os eventos estudados e quando analisa fenômenos contemporâneos em profundidade e em seu contexto de vida real.

Os estudos de caso têm um lugar diferenciado na pesquisa qualitativa, existem para pelo menos quatro aplicações diferentes. Primeiro, explicar os presumidos vínculos causais nas intervenções da vida real que são demasiados complexos para as estratégias de levantamento. Segundo, descrever uma intervenção e o contexto da vida real no qual ela ocorreu. Terceiro, ilustrar determinados tópicos em uma avaliação. E, por fim, explorar as situações em que a intervenção sendo avaliada não possui um único e claro conjunto de resultados (Yin, 2010, p. 41).

Um erro fatal na realização dos estudos de casos é conceber a generalizações estatísticas dos resultados, quando os estudos de casos não são "unidades de amostragem (Yin, 2010).

> *Os estudos de casos permitem generalizações analíticas, em que uma teoria previamente desenvolvida é usada como um padrão, com o qual são comparados os resultados empíricos dos estudos de caso. Se dois ou mais casos demonstram apoiar a mesma teoria, a replicação pode ser afirmada.* (Yin, 2010, p. 61)

As conclusões analíticas tornam-se mais robustas e poderosas quando provenientes de dois ou mais estudos de casos. (Yin, 2010) recomenda que, sempre que possível, se prefira os projetos de casos múltiplos, porque os benefícios analíticos são substanciais e há a possibilidade de replicação direta.

A definição das questões de pesquisa é provavelmente o passo mais importante a ser dado no processo de pesquisa, porque proporciona uma indicação importante para o método de pesquisa a ser usado e orienta a coleta e a análise de dados (Yin, 2010).

Para a presente pesquisa, face ao problema de base identificado e tendo em conta a revisão de literatura efetuada, identificaram-se as seguintes questões de pesquisa:

1. Como as organizações públicas implementam as práticas de gestão de riscos?
2. Quais as percepções sobre a gestão de riscos nas organizações públicas?
3. Como a auditoria interna pode ajudar a projetar, desenvolver e implementar políticas e práticas de gestão de riscos no setor público?
4. Quais são os direcionadores para a implementação de uma gestão de riscos bem-sucedida?

Assim, considerando as questões de pesquisa e a natureza do fenómeno estudado, optou-se pela realização de estudos de casos múltiplos como estratégia de investigação neste trabalho.

3.2. Método de coleta de dados

A evidência do estudo de caso pode vir de várias fontes, como documentação, registros em arquivo, entrevistas, observação direta, observação participante, artefatos físicos, dentre outros (Yin, 2010). Considerando o propósito da presente investigação, a documentação e a entrevista foram as fontes de informação utilizadas.

Para os estudos de caso, o uso mais importante dos documentos é para corroborar e aumentar a evidência de outras fontes. Devido ao seu valor global, os documentos desempenham um papel explícito em qualquer coleta de dados na realização de estudo de casos (Yin, 2010, p. 130). Como fonte complementar de evidência, o presente estudo coletou documentos das organizações estudadas, disponíveis publicamente na Internet, como a política e a metodologia de gestão de riscos da organização, a versão do último relatório de gestão publicado da organização e, quando aplicável, as normas referentes ao modelo de governança da instituição.

As entrevistas constituem uma das fontes mais importantes de informação para o estudo de caso. (Yin, 2010) recomenda o uso de entrevistas em profundidade, em que se pergunta aos atores-chave sobre os fatos de um assunto, suas opiniões sobre os eventos, ou, até mesmo, pede-se ao entrevistado que proponha seus próprios insights para determinada situação. Há também a entrevista focada, que embora seja também conversacional, há de ser seguido um conjunto de questões.

Assim, em consonância às observações do autor, na presente pesquisa as perguntas foram formuladas de modo a satisfazer as necessidades da linha de investigação e, simultaneamente, apresentar questões "amigáveis" (Yin, 2010).

Quadro 5 – Exemplos de perguntas aplicadas às entrevistas

Fale um pouco sobre o processo de gestão de riscos da sua organização
Considera que as informações produzidas pela área de riscos abordam os riscos mais críticos da organização?
Quais sugestões faria à Auditoria Interna para melhorar ainda mais seu trabalho de asseguração da gestão de riscos da organização?
Como avalia o processo de gestão de riscos da sua organização?
Se fosse implantar uma área de gestão de riscos em uma nova organização como começaria? O que seria prioritário?

Fonte: elaboração própria

Embora as entrevistas sejam uma fonte essencial de evidência do estudo de caso, elas apresentam desvantagens. Pode haver parcialidade da resposta devido às questões mal articuladas, incorreções devido à falta de memória do respondente, reflexividade do entrevistado em responder o que o entrevistador quer ouvir (Yin, 2010, p. 129).

Esses pontos fracos precisam ser observados e mitigados. Para tanto, Yin (2010) recomenda que se empreguem múltiplas fontes de evidência em relação ao mesmo fenômeno; a construção de uma base de dados, através de notas, documentos, tabulações e narrativas (interpretações e descrições dos eventos observados, registrados etc.); estabelecimento de uma cadeia de evidências, que possibilite ao leitor a percepção de evidências capazes de legitimar o estudo, desde as questões de pesquisa até as conclusões finais.

A principal vantagem do uso de múltiplas fontes de evidência é o desenvolvimento de linhas convergentes de investigação, um processo de triangulação e corroboração. Desta feita, qualquer achado ou conclusão do estudo de caso é, provavelmente, mais convincente e acurado (Yin, 2010, p. 143).

Em linha com essas orientações, algumas medidas foram adotadas para mitigar os riscos associados ao método escolhido: a) empregou-se múltiplas fontes de evidência, a partir da aplicação da entrevista a diferentes atores dentro de uma mesma organização e

a diferentes modelos organizacionais; b) elaborou-se guiões de perguntas para cada tipo de entrevistado; c) fez-se teste-piloto a fim de validar o roteiro e testar as habilidades do entrevistador.

Os guiões permitiram focalizar as entrevistas no assunto em análise, ainda que procurando manter as questões abertas e os entrevistados livres para responder e abordar outros temas correlatos. Os objetivos estabelecidos para cada grupo de pergunta estão descritos no quadro seguinte.

Quadro 6 -Relação de objetivos para as entrevistas

Chefe da área de riscos
• Levantar o perfil profissional do chefe e da estrutura da área de riscos • Mapear o atual processo de gestão de riscos da organização; e explorar aspectos históricos relevantes da implementação da gestão de riscos • Mapear a relação da área de riscos com a alta administração e demais gestores • Mapear a relação da área de riscos com a auditoria interna (quando aplicável) • Mapear a relação da área de riscos com a Assessoria Especial de Controle Interno (quando aplicável) • Identificar em que papel a CGU atuou ou pode atuar na Gestão de Riscos da organização • Levantar pontos de melhoria do atual processo de Gestão de Riscos da organização • Levantar contribuições para implementar o processo Gestão de Riscos em uma nova organização
Integrante da alta Gestão
• Levantar o perfil profissional do entrevistado • Mapear a atuação do Comitê de Governança no processo de Gestão de Riscos da organização • Avaliar a relação do Comité de Governança com a área de riscos (se houver): • Avaliar a participação do AECI (se houver) na Gestão de Riscos • Avaliar a atuação da auditoria interna (se houver) na Gestão de Riscos da organização • Avaliar a atuação da CGU na Gestão de Riscos da organização • Levantar pontos de melhoria do atual processo de Gestão de Riscos da organização

Fonte: elaboração própria

Para (Yin, 2010) o treinamento do investigador é essencial para assegurar as habilidades desejadas para extrair do caso as informações relevantes; é desejável que o investigador seja capaz de formular boas questões, para ter boas respostas; seja bom ouvinte e flexível, sem perder o rigor; ter bom conhecimento sobre os temas estudados. E, sempre que possível, é esperado que se faça estudos de caso-piloto para antecipar alguns ajustes na pesquisa, se necessário. Desta feita, realizou-se uma entrevista-piloto a um

Assessor Especial de Controle Interno, também responsável pela área de gestão de riscos do seu ministério. A entrevista aconteceu em dezembro e teve a duração de 55 minutos. Os dados desta entrevista não foram utilizados no resultado da pesquisa, mas serviu para treinar o entrevistador, avaliar a pertinência, a cronologia e duração das perguntas.

Após o refinamento dos guiões, passou-se para a etapa do trabalho de campo. As entrevistas ocorreram nos meses de dezembro de 2022 e janeiro de 2023, de modo online, utilizando a plataforma Microsoft Teams e foram todas gravadas, a partir do consentimento expresso do entrevistado, para posterior transcrição e análise dos dados. Ao total foram 9 (nove) entrevistas, de 6 (seis) organizações, no tempo total de 9h25min, com duração média de 1 (uma) hora.

3.3. Universo e unidades de análise

A seleção de casos a serem estudados trouxe o desafio de definir aqueles de melhor representatividade para a investigação, uma vez que o universo do setor público pode ser definido de várias formas, de acordo com os tipos ou natureza da organização e o nível da estrutura governamental. Meio a este desafio, mas atento ao objeto de estudo da presente pesquisa, adotou-se como referência primária o levantamento realizado pelo TCU para o Índice Geral de Governança do Setor Público (iGG) de 2021 (BRASIL, 2021). A seleção das organizações considerou os seguintes critérios. Primeiro, aquelas organizações com o nível de maturidade aprimorado (70,01% a 100%) para prática “Gerir riscos (2110)”, de modo a contemplar organizações que, a partir do relato da sua trajetória de implantação da gestão de riscos, pudessem contribuir com informações relevantes para responder aos objetivos da pesquisa, especialmente quanto aos fatores indutores e dificultadores da implementação da gestão de riscos organizacional.

O segundo critério considerou o arranjo organizacional das unidades. A seleção contemplou instituições da administração indireta com unidades próprias de auditoria interna, e órgãos da administração direta sem unidades próprias de auditoria interna, de modo a coletar informações de diversos cenários sobre a atuação da unidade própria de auditoria interna, dos AECIs e da CGU enquanto unidade de auditoria interna

governamental na implementação da gestão de riscos organizacional para diferentes arranjos.

E, por fim, o terceiro fator contemplou a seleção apenas das organizações do Poder Executivo federal. Assim, após a aplicação desses critérios, o universo passou de 378 unidades para 89 unidades, distribuído como consta do quadro seguinte.

Quadro 7 – Universo adaptado das entidades do Poder Executivo Federal do Brasil

Administração Direta	Administração Indireta
Nível Aprimorado (11 organizações) •4 Ministérios •1 Forças Armadas •1 Segurança Pública •5 Outras	Nível Aprimorado: 78 unidades •30 Autarquias •15 Empresas Públicas •11 Fundações Públicas •22 Sociedade de Economiga Mista

Fonte: Elaboração própria

Para que os dados recolhidos permitissem obter visões diferentes sobre aspectos relevantes do processo de implementação da gestão de riscos dentro de cada contexto organizacional, as entrevistas tiveram como público-alvo os chefes da área de risco, assessores especiais de controle interno e representantes da alta administração.

A partir deste universo de entidades e dos critérios adotados, as organizações foram selecionadas com base num processo de amostragem intencional, considerando a facilidade de acesso da pesquisadora às potenciais organizações. Das 78 organizações da administração indireta, foram escolhidas três; e das 11 da administração direta foram selecionados três ministérios. O quadro a seguir apresenta a área temática, a natureza jurídica e o nível de maturidade das organizações selecionadas:

Quadro 8 - Mapa das organizações selecionadas por área temática x natureza jurídica

Área Temática	Órgão Público	Autarquia	Empresa Pública	Nível de maturidade
Auditoria	X			0,87
Regulação da Política Fiscal e Monetária		X		0,92
Infraestrutura	X			0,85
Regulação em Saúde		X		0,85
Segurança Pública	X			0,87
Tecnologia da Informação			X	1,00
TOTAL	**3**	**2**	**1**	

Fonte: elaboração própria

3.4. Método de Análise dos Dados

Para (BARDIN, 2013, p. 121) as diferentes fases de análise de conteúdo organizam-se em torno de três pólos cronológicos: 1) pré-análise; 2) exploração do material; 3) tratamento dos resultados, a inferência e a interpretação (ver item 4 a seguir).

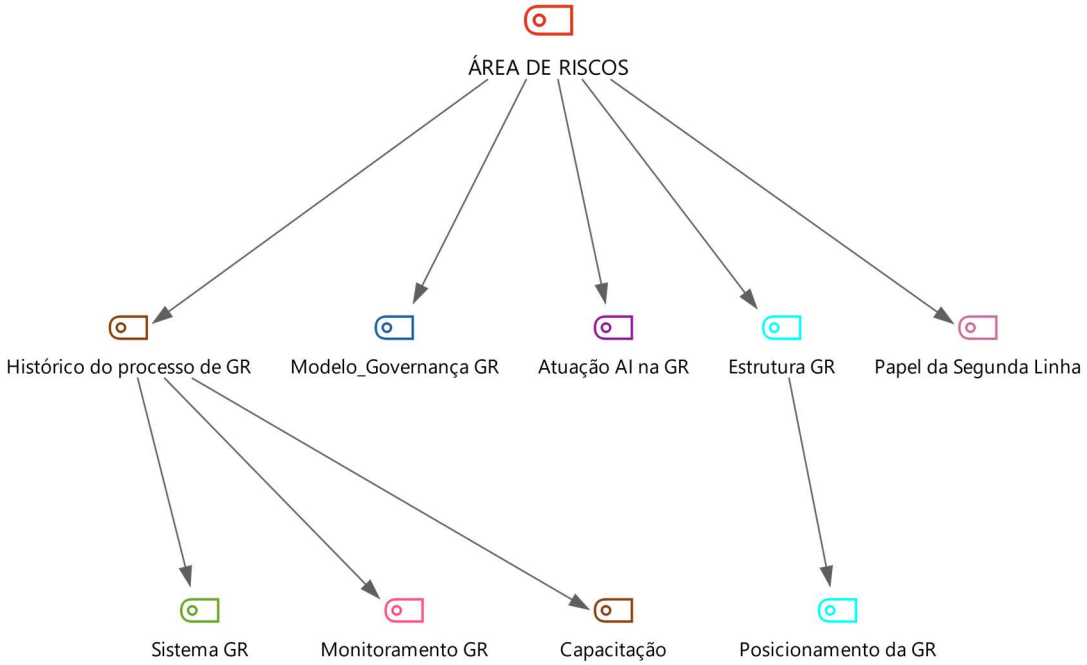
3.4.1. Pré-análise

É a fase de organização propriamente dita e pode variar a depender do tipo de material a ser analisado e da forma como foi coletado (BARDIN, 2013). Assim, considerando as entrevistas realizadas na etapa de coleta de dados, como principal fonte de dados da pesquisa, esta etapa envolveu as seguintes atividades:

1. Transcrição das entrevistas gravadas, com a ajuda do software Reshape;
2. Importação das transcrições das entrevistas para o software MaxQDA;
3. Organização dos arquivos de modo a facilitar o trabalho de análise;
4. Leitura flutuante de algumas das entrevistas a fim de estabelecer o primeiro contato com os documentos a analisar; e
5. Montagem da estrutura de códigos no MaxQDA, de acordo com as questões de pesquisa:

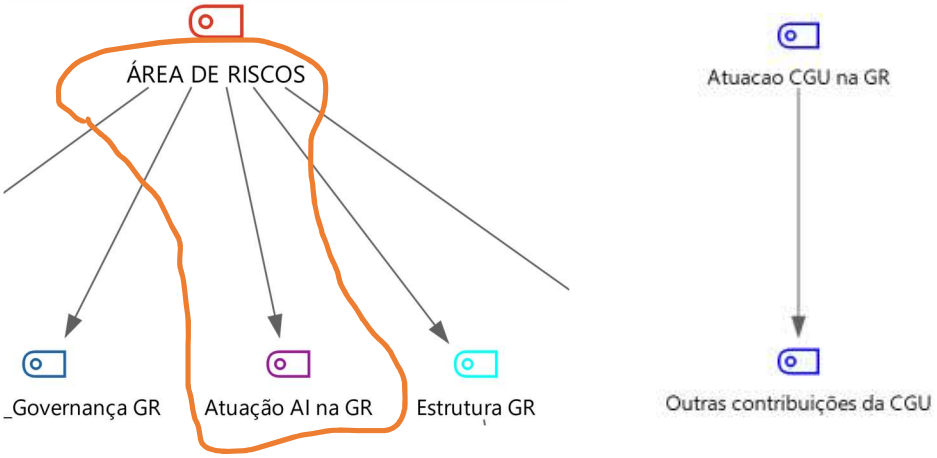
Quadro 9 -Questões de pesquisa e respectivas categorias

1. Como as organizações públicas implementam as práticas de gestão de riscos?



2. Quais as percepções sobre a gestão de riscos nas organizações públicas?

3. Como a auditoria interna pode ajudar a projetar, desenvolver e implementar políticas e práticas de gestão de riscos no setor público?



4. Quais são os direcionadores para a implementação de uma gestão de riscos bem-sucedida?

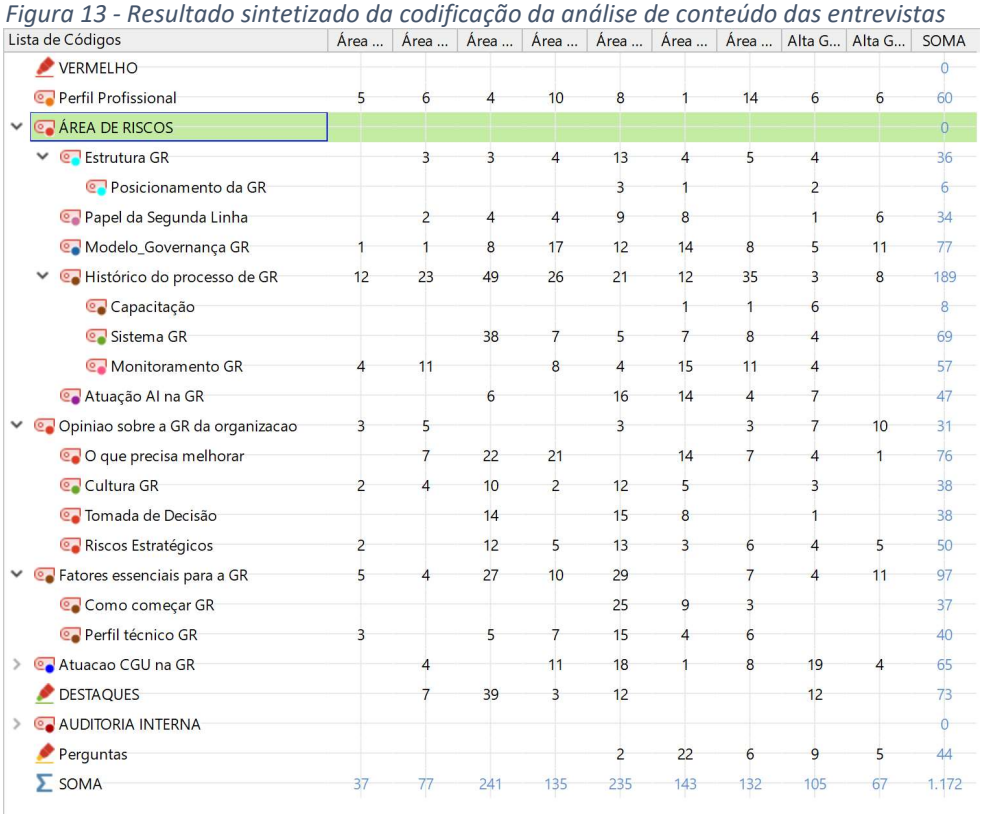
Fonte: elaboração própria, com apoio do software MaxQDA

3.4.2. Exploração do material

É a fase que se consubstancia essencialmente em operações de codificação, decomposição ou enumeração, em função de regras previamente estabelecidas. A codificação transforma o dado bruto em uma representação de conteúdo, a partir do recorte do dado, classificação e agregação desse recorte em categoria (BARDIN, 2013).

Esta etapa consistiu em codificar os dados, segundo as categorias previamente definidas, com a ajuda do MaxQDA e depois um refinamento em planilhas Excel. Ao total, foram codificados 1.172 trechos das nove entrevistas realizadas no software MaxQDA, conforme figura a seguir.

Figura 13 - Resultado sintetizado da codificação da análise de conteúdo das entrevistas



Lista de Códigos	Área ...	Área ...	Área ...	Área ...	Área ...	Área ...	Área ...	Alta G...	Alta G...	SOMA
VERMELHO										0
Perfil Profissional	5	6	4	10	8	1	14	6	6	60
ÁREA DE RISCOS										0
Estrutura GR		3	3	4	13	4	5	4		36
Posicionamento da GR					3	1		2		6
Papel da Segunda Linha		2	4	4	9	8		1	6	34
Modelo_Governança GR	1	1	8	17	12	14	8	5	11	77
Histórico do processo de GR	12	23	49	26	21	12	35	3	8	189
Capacitação						1	1	6		8
Sistema GR			38	7	5	7	8	4		69
Monitoramento GR	4	11		8	4	15	11	4		57
Atuação AI na GR			6		16	14	4	7		47
Opiniao sobre a GR da organizacao	3	5			3		3	7	10	31
O que precisa melhorar		7	22	21		14	7	4	1	76
Cultura GR	2	4	10	2	12	5		3		38
Tomada de Decisão			14		15	8		1		38
Riscos Estratégicos	2		12	5	13	3	6	4	5	50
Fatores essenciais para a GR	5	4	27	10	29		7	4	11	97
Como começar GR					25	9	3			37
Perfil técnico GR	3		5	7	15	4	6			40
Atuacao CGU na GR		4		11	18	1	8	19	4	65
DESTAQUES		7	39	3	12			12		73
AUDITORIA INTERNA										0
Perguntas					2	22	6	9	5	44
SOMA	37	77	241	135	235	143	132	105	67	1.172

Fonte: elaboração própria, com apoio do software MaxQDA

O detalhe das etapas de codificação no MAXQDA e no Excel está demonstrado no Anexo I.

4. CAPÍTULO III - RESULTADOS E DISCUSSÃO

4.1. Apresentação dos Resultados

Preliminarmente, antes de discorrer sobre os resultados encontrados, apresenta-se neste tópico as características da área de riscos das organizações entrevistadas. Tendo em vista o objetivo deste trabalho, considera-se área de riscos aquelas unidades que executam dentro da estrutura organizacional as funções de prover aconselhamento e expertise complementar, treinamento, facilitação na implementação de modelos/processos de risco, melhoria contínua das práticas de gestão de riscos, dentre outras funções correlatas (Barrett AO, 2014; IIA, 2020).

Em relação ao posicionamento organizacional das unidades de gestão de riscos, notou-se que nos ministérios, a função estava sob a responsabilidade da Assessoria Especial de Controle Interno (AECI), à exceção de ORG6, que por suas características não possui a estrutura da AECI, ao passo que para as organizações da administração indireta a função encontrava-se dentro do quarto nível hierárquico, sem prejuízo da sua atuação, uma vez estavam em diretorias que integravam a estrutura máxima de governança da organização. Além disso, os chefes dessas unidades de riscos relataram que faziam *report* periódico à alta administração sobre a gestão de riscos organizacional.

Em termos de tamanho das equipes, das seis organizações entrevistadas apenas uma apresentou uma equipe com mais de seis membros. A quantidade de integrantes ficou entre 3 e 5 pessoas, incluindo o chefe da área de riscos. Observou-se que todos os chefes entrevistados eram servidores e empregados públicos de carreira e apresentavam grande período de experiência, quer seja na temática de riscos ou nas atividades finalísticas da organização. O tempo médio na carreira pública foi de mais de 20 anos.

Em relação à qualificação, o perfil técnico dos integrantes da área de riscos, por regra, apresentou-se muito qualificado, tanto para o chefe da unidade, quanto para os demais componentes da equipe.

4.1.1. Como as organizações públicas implementam as práticas de gestão de riscos?

Este tópico aborda os principais pontos levantados nas entrevistas e nas análises dos documentos publicados pelas organizações estudadas. Os vários aspectos levantados referem-se a dados atuais, mas com referências históricas, no que couber, de modo a apresentar também informações relevantes sobre os desafios enfrentados pelas organizações no decorrer do seu processo de implementação. A tabela a seguir sintetiza algumas características deste processo.

Quadro 10 - Características do processo de gestão de riscos das organizações

ASPECTOS	ORG1	ORG2	ORG3	ORG4	ORG5	ORG6
Tipologia	Adm. Indireta	Adm. Indireta	Adm. Direta	Adm. Direta	Adm. Indireta	Adm. Direta
1ª Política de Gestão de Riscos	2014	2011	2017	2019	2016	2017
Área de Riscos (2ª linha)	Assessoria de Riscos	Departamento de Riscos	Assessoria Especial de Controle Interno	Assessoria Especial de Controle Interno	Departamento de Riscos	Escritório de Riscos e Processos
Modelo para a metodologia de gestão de riscos	ISO 31000 COSO ERM	ISO 31000 COSO-ERM	ISO 31000 COSO-ERM	COSO - ERM	ISO 31000	ISO 31000 COSO-ERM
Sistema de TI para Gestão de Riscos	Não há sistema de TIC.	Sistema próprio	Sistema próprio	Sistema aberto	Sistema contratado	Sistema próprio
Declarado o apetite a riscos?	Em estudo	Sim	Sim	Sim	Sim	Em estudo
É feita a gestão de riscos estratégicos?	Em desenvolvimento	Sim	Sim	Sim	Sim	Em desenvolvimento

Fonte: elaboração própria

Muito embora algumas das organizações já possuíssem estruturas específicas de gestão de riscos para determinados negócios da organização, o aspecto considerado para a institucionalização do processo de gestão de riscos organizacional foi a publicação da primeira Política de Gestão de Riscos (PGR).

A estrutura de governança interna de gestão de riscos estabelecida pelas organizações pesquisadas, por meio da sua PGR, tem como instância máxima um colegiado composto pelos dirigentes máximo e pelos executivos ligados diretamente a ele e, embora a sua denominação variasse em algumas organizações, as competências atribuídas a esse comitê estão de acordo com a IN Conjunta MP/CGU nº 1, de 2016.

Para iniciar a gestão de riscos, as ORG3 e ORG4 iniciaram os seus processos de implantação pelos riscos estratégicos porque precisavam convencer a alta administração dos benefícios diretos da gestão de riscos. Para os chefes da área de riscos - os AECIs, iniciar a gestão de riscos por processo era muito lenta e a percepção dos benefícios para a alta gestão demandava muito tempo. Além disso, o processo iniciou sem nenhum sistema de TIC, portanto, operar planilhas e ferramenta de BI era mais simples para os riscos estratégicos, que eram em menor número, do que para os riscos de processo.

> *"A gente está assessorando o ministro e a gente sabe que a governança vem desse planejamento[estratégico](...). E ele [processo de gestão de riscos] vinculado à cadeia de valor, vinculado aos objetivos estratégicos, até porque essa foi a primeira decisão que a gente tomou também, se não a gente não daria conta." (ORG3)*
>
> *"O primeiro movimento que a gente teve foi aproximar a gestão de risco dos projetos estratégicos. Então, era uma tabela a ser preenchida no roteiro dos projetos estratégicos. Depois a gente tentou aproximar dos processos e viu que os processos eram muitos numerosos." (ORG3)*
>
> *"Quando fez a revisão em 2019 do planejamento estratégico que a gente herdou em 2018, o Ministério aqui já largou com risco estratégico. Antes de a gente ter o método escrito para gerir risco em processo de trabalho, o estratégico já nasceu com a própria estratégia. Então já nasceram os primeiros BIs para acompanhamento, a lógica de monitoramento, de acompanhamento da estratégia" (ORG4)*
>
> *"não é um cardápio muito grande, é uma característica até do risco estratégico, você tem um portfólio relativamente pequeno em relação a risco em processo de trabalho" (ORG4)*

Na etapa de avaliação dos riscos pelas unidades internas das organizações, o método escolhido foi o *Self-Assessment,* onde cada gestor e sua equipe fazem a avaliação de riscos dos objetos (processos, projetos, políticas, etc.) de sua responsabilidade. Desse modo, as unidades de riscos promoviam treinamentos para capacitar as pessoas designadas pelos gestores das unidades e o suporte na etapa de avaliação e criação do plano de tratamento dos riscos.

> *"Optou-se pelo modelo da autoavaliação (self-assessment). Assim, cada área faria sua própria avaliação de riscos, ficando a cargo da área de riscos a capacitação dos servidores para esta atividade." (ORG1)*
>
> *"A metodologia empregada para os riscos operacionais é o Self Assessment feito pelos departamentos, sob a supervisão da área de riscos." (ORG2)*
>
> *"A unidade faz [mapeamento dos riscos], a gente dá suporte para ela, a gente dá treinamento." (ORG3)*
>
> *"Outra dimensão de risco que nós temos aqui, que seriam riscos operacionais e de projeto, esses daí é tudo feito pela primeira linha, com a nossa supervisão." (ORG5)*

Para selecionar os processos a serem avaliados o método variou entre as organizações, de acordo com os recursos disponíveis no início da implementação da gestão de riscos e com os objetivos esperados para os primeiros mapeamentos de riscos. A ORG1, por exemplo, que adotou a estratégia de iniciar a gestão de riscos por processo, quando iniciou a implementação não possuía informações sobre os seus processos. Como não havia um mapa de processos, coube aos gestores selecionar um processo para iniciar a avaliação de riscos. A orientação dada pela área de riscos foi de selecionar os processos mais simples da unidade, porque eles serviam para formar uma curva de aprendizagem.

> *A nossa sugestão é que comece por um processo menos complexo, que é para você ter sua curva de aprendizagem. Se você começar num processo mais complexo para mostrar resultado, provavelmente você não vai mostrar resultado, você não vai chegar no final e vai se bloquear para a avaliação de risco. Aprenda primeiro o que é, para você saber o quanto você precisa de esforço, para aí sim, quando tiver sua curva de aprendizagem, você passar a ter processos mais complexos. (ORG1)*

No outro extremo, a ORG3, que iniciou a implementação da gestão de riscos pelos riscos estratégicos, estabeleceu que as unidades iniciassem o mapeamento pelo processo/projeto/programa mais crítico da unidade, para que a informação já gerasse valor para a supervisão ministerial.

> *"A gente pegou o processo mais complicado que tinha, mais difícil que tinha para começar." (ORG3)*
>
> *"Então, não adianta eu ficar fazendo uma área que não representava muita coisa, então era uma política que tinha uma certa representatividade. Encaminhávamos no ofício uma relação de políticas vinculadas aos objetivos estratégicos para eles. E já*

> *sinalizávamos para eles que obrigatoriamente essa aqui eu vou fazer, tem que fazer." (ORG3)*

Observou-se que ao longo dos anos as organizações aprimoraram os seus métodos de avaliação, a exemplo da ORG2 que, além do *self assessment*, utiliza atualmente como fonte de informações o registro de incidentes; e para processos mais específicos e relevantes, os indicadores de riscos. A ORG1 implantou a arquitetura de processo e criou o seu mapa de processos prioritários para avaliação de riscos.

As organizações evoluíram também em mecanismos para permitir a integração da gestão de riscos à estratégia e aos processos organizacionais. A ORG3, por exemplo, sistematizou o seu processo de avaliação de riscos atrelado às alterações dos elementos do planejamento estratégico e, mais recentemente, à sua carteira de políticas públicas.

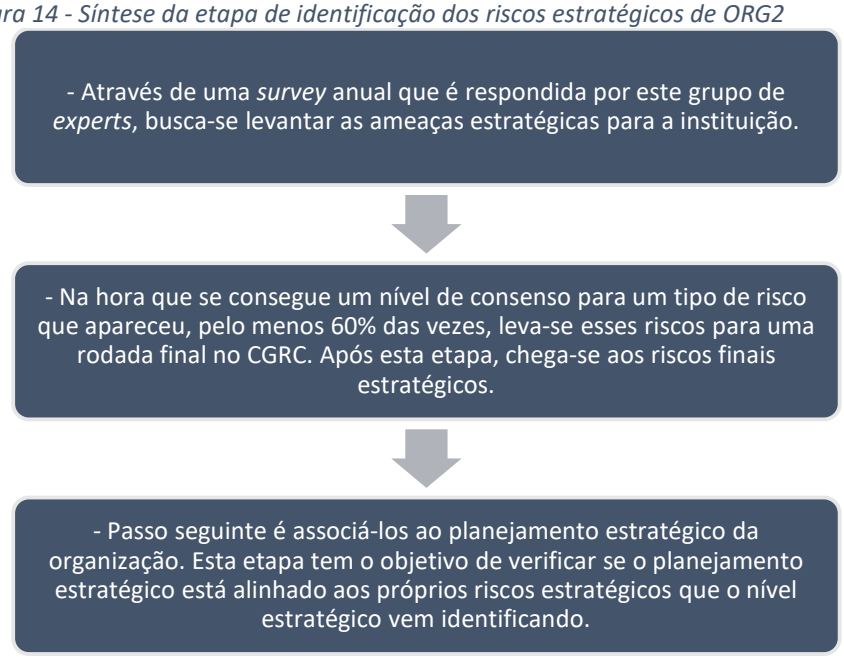
> *É uma metodologia que acompanha o planejamento estratégico porque é a definição dos processos de trabalho prioritário. Ela é feita pela vinculação da cadeia de valor, dos indicadores e projetos estratégicos. (ORG3)*
>
> *Para você só ter ideia, algumas políticas foram incluídas agora recentemente, e já entraram nas atividades de implementação do gerenciamento de risco. Então eles já trabalharam no processo, não precisou nem de eu fazer reunião (...). Ou seja, virou uma rotina. (ORG3)*
>
> *Então cada vez que um gestor de um processo operacional declara seus objetivos, a gente pede para ele fazer gestão de risco em cima desses objetivos. (ORG5)*

No tocante à metodologia empregada para gestão dos riscos estratégicos, as organizações estudadas adotaram modelos e dinâmicas diferentes. Na ORG5, por exemplo, os riscos estratégicos são mapeados pelos gestores, com o suporte direto da área de riscos, mas o monitoramento e o *report* são feitos diretamente pela área de riscos.

> *"A gente puxa o telefone e marca uma reunião com cada gestor de risco estratégico aqui, geralmente eles são diretores e superintendentes, e a cada três meses um agente, a gente chama de agente de segunda linha ou agente corporativo, vai ligar e vai fazer o monitoramento como se fosse primeira linha." (ORG5)*

Para identificar os riscos estratégicos, a ORG2 adotou uma abordagem específica, denominada de "consenso de experts", que são pessoas posicionadas em níveis estratégicos da organização. O fluxo relatado para esta etapa, pode ser assim resumido:

Figura 14 - Síntese da etapa de identificação dos riscos estratégicos de ORG2



Fonte: entrevista da área de riscos da ORG2

Nessa mesma linha, a ORG6 tem o entendimento de que o risco estratégico é muito difuso, existem muitas ameaças que são externas e que, portanto, não é possível alcançá-las via mapeamento de processo. A metodologia empregada para os riscos estratégicos pela ORG6, baseada na metodologia ágil, estava em fase de teste e ainda não estava institucionalizada, segundo informações do entrevistado da organização.

Após as etapas de identificação e avaliação dos riscos, têm-se as etapas de monitoramento e de comunicação. De forma resumida, a tabela a seguir apresenta o fluxo e periodicidade dos *reports* às instâncias de governança das organizações pesquisadas:

Quadro 11 - Síntese do processo de monitoramento e comunicação dos riscos organizacionais

Organização	**Monitoramento e Comunicação**
ORG1	- a cada dois meses o mapa de todos os riscos da organização é apresentado na reunião do Comitê de Governança, Riscos e Controle. - Em geral, os responsáveis pelos riscos mais relevantes participam das reuniões a convite dos diretores.
ORG2	- monitoramento trimestral com *report* para a Diretoria Colegiada - área de riscos consolida toda a informação e indica para a Diretoria Colegiada os aspectos mais relevantes - quando demandada pela alta gestão, a área de riscos faz o monitoramento e *report* diário de algum risco específico. Neste caso a análise é menos analítica.

Organização	Monitoramento e Comunicação
ORG3	- Nas reuniões mensais do comitê de governança é levado todo o plano de tratamento dos riscos, mas é dado destaque para questões relevantes como, por exemplo, os riscos que são extremos, os prazos que estão sendo vencidos, etc. - há o relatório semestral de monitoramento do processo de gerenciamento de risco do ministério e de todas as suas unidades vinculadas
ORG4	- há dois grandes blocos de Reuniões de Acompanhamento da Estratégia (RAE) – RAE's setorial e RAE ministerial. - os riscos estratégico são repassados nessas RAE's. Os líderes de programa elencam os riscos de maior criticidade, de maior severidade, para serem tratados nessas reuniões. - quadrimestralmente são elaborados relatórios detalhados para poder discutir e trabalhar nas instâncias de governança.
ORG5	- monitoramento trimestral com *report* para cada diretoria - monitoramento semestral com *report* para a diretoria colegiada, conselho de administração, comitê de auditoria e conselho fiscal - a área de riscos faz o monitoramento direto dos riscos estratégicos e dos riscos de processos e de projetos avaliados como alto ou muito alto.
ORG6	- a área de riscos gera relatórios gerenciais de monitoramento para subsidiar a atuação tanto do Comitê de Governança, quanto do Comitê Gerencial. - as reuniões do Comitê Gerencial ocorrem, no mínimo, a cada 3 meses. - nas Reuniões de Avaliação Estratégica com o Comitê de Governança, a diretoria de governança, mesmo sem voto, está presente e leva a temática gestão de riscos para essas reuniões.

Fonte: elaboração própria

Para apoiar o processo de supervisão e de monitoramento da gestão de riscos organizacional observou-se que as organizações pesquisadas utilizaram os agentes de riscos (AGR) e os comitês gerenciais em níveis tático e operacional para atuarem no apoio às diversas etapas da gestão de riscos, tal como nas atividades de identificação, avaliação, supervisão e monitoramento dos riscos dentro das unidades de negócio da organização ou entre elas quando a alçada de riscos extrapolavam as competências de uma única unidade:

> *"cada área, tem nomeado pelo menos um AGR, que é um agente de gestão de risco, e esse agente é a nossa porta de entrada nos diversos departamentos." (ORG2)*
>
> *"Ela [unidade interna do ministério] monta o plano de implementação [plano de tratamento do riscos], encaminha via sistema para AECI que (...) é submetido ao comitê de gestão de risco. A gente faz essa discussão no comitê de gestão de risco. (...) ou discute com as pessoas*

> *de novo para dar uma melhorada, ou submete para o comitê de governança estratégica que aprova." (ORG3)*
>
> *"No nível tático, a gente tem um comitê técnico de governança e aí é formado por DAS 4 e 5 de várias áreas, ou melhor, de todas as áreas do ministério, tanto área meia quanto área finalista. Então são atribuições, muitas das vezes, para tratar os próprios riscos de processo de trabalho que muitas das vezes começam a ficar fora da alçada do gestor do próprio risco." (ORG4)*
>
> *"então o comitê setorial serve pra ajudar o diretor a tomar decisões de gestão de risco dentro de qualquer ponto do processo. (...) o comitê pode discutir identificação de risco, pode discutir avaliação de risco, pode discutir monitoramento." (ORG5)*

O esforço empreendido pelas unidades de riscos para produzir informações úteis para o processo de monitoramento e de comunicação variou consideravelmente entre as organizações, consoante os recursos humanos e as ferramentas disponíveis. A ORG1 e a ORG4, que não possuíam sistemas próprios de gestão de riscos, relataram a dificuldade e o tamanho do esforço em consolidar as informações de riscos para gerar painéis gerenciais e relatórios de monitoramento consolidados, assim como, em supervisionar o processo de implementação dos controles para os riscos mapeados, tendo em vista o atual volume de dados para tratar e consolidar. A necessidade de um sistema de TIC adequado foi apontada como item fundamental para aumentar a eficiência da gestão de riscos da organização.

> *"Passado o tempo, (...) tem muita informação, já tem muito trabalho feito e realmente agora um sistema está fazendo falta. (...) Porque eu preciso depois tabular essas informações que estão no Excel para poder gerar os relatórios. Então, assim, a primeira, a principal coisa que a gente precisa, a principal ferramenta, seria um sistema." (ORG1)*
>
> "Justamente a parte onde você, onde os gestores estruturam os seus planos de ação. A par*tir dali o sistema de fato não ajuda na questão do monitoramento." (ORG4)*

No outro extremo está a ORG2 que possui um sistema próprio de TIC integrado às diversas etapas do processo de gestão de riscos e com outros sistemas da organização, com ganhos diretos para os servidores e gestores dos departamentos, para a área de riscos e ainda para a auditoria interna.

> *"da dimensão de métodos e metodologias, a gente usa muita automação nisso, o que facilita bastante você fazer um pouquinho mais com recursos humanos limitados."*
>
> *"Então, pelo menos esse cara[AGR] tem acesso ao sistema, (...) aonde ele consegue registrar incidentes, aonde ele consegue fazer o RCSA (...)*

> *e isso tudo alimenta esse mesmo sistema que a gente consolida aqui na área de risco."*
>
> *"na fase de planejamento, nós já temos acesso às informações da área de risco. É um relatório que ele já disponibilizou para nós, para que a gente possa extrair e executar todos os testes que a equipe achar que deve fazer. Inclusive utilizar os riscos que já estão mapeados lá para fazer o nosso trabalho, fazer os testes de controle."*

Como dimensão essencial à implementação da gestão de riscos, mapeou-se também as principais ações utilizadas pelas organizações para o fomento da cultura de riscos. Verificou-se que as ações estavam relacionadas à comunicação contínua dirigida a servidores e funcionários da organização, em níveis de complexidades diferentes a depender do público-alvo; à capacitação contínua dos gestores de riscos e agentes de riscos; e ao desenvolvimento de ferramentas práticas para facilitar o trabalho dos gestores na gestão de riscos.

> *"Então a gente tem gente que não sabe nada de risco, nem de conformidade, (...) a gente tem um plano de comunicação com eles, que é para fazer aculturamento neles, para acender a chama do que é gestão de risco, falando bem para leigo mesmo, a gente faz brincadeira, faz palavra cruzada, tentando agora fazer um joguinho de palavra cruzada, uma coisa assim para entretenimento." (ORG5)*
>
> *"Eu acho que a gente precisa melhorar é a compreensão das pessoas sobre o que é gestão de risco, e isso leva muito tempo. Isso não acontece de uma hora para outra. E a história é você estar o tempo inteiro dizendo, falando sobre o assunto. Precisa muito conversar o tempo inteiro sobre o assunto, estar fomentando o tempo inteiro." (ORG3)*
>
> *"Outros recursos que se complementam, de tempos em tempos, reunir os AGRs para discutir os riscos emergentes, focar nas revisões de risco, discutir com os principais stakeholders da ação de risco, dentre outras." (ORG2)*
>
> *"Durante todo esse processo a gente entendeu que é importante chegar nas áreas já com ferramentas mais práticas e adequadas para não onerar tanto o trabalho dos servidores." (ORG6)*

Outro elemento apontado como relevante para o aculturamento do corpo funcional da organização foi a estabilidade e qualificação do corpo funcional. Nas organizações onde há uma rotatividade grande de gestores e servidores, notou-se um esforço maior no aculturamento.

> *"O ministério tem uma certa rotatividade de servidores, muitas das vezes servidores não estão vindo de locais anteriores em que o assunto estava mais ou menos no mesmo nível de maturidade, muitas das vezes estava muito embrionário de onde ele veio, então ele precisa se aculturar aqui com outra realidade, então isso também traz um certo atraso, digamos assim, da velocidade que a gente gostaria de imprimir, mas tem seguido adiante, a gente está avançando." (ORG4)*

> *"Eu cansei de fazer reuniões iniciais, porque a gente passou por um período que eu conversava com o secretário hoje, passava 2 meses, já era outro secretário, eu tinha de voltar lá e conversar com o novo secretário e falando desse processo todo, ou seja, da necessidade de todos estarem envolvidos." (ORG3)*

Por fim, em relação à declaração do apetite a riscos, embora mais da metade tenha o seu apetite a risco definido, apenas a ORG2 deixou evidente que o apetite a riscos era base para medição e referência para o trabalho de supervisão feito pela área de riscos (segunda linha) e *report* às instâncias de governança.

> *"O apetite a riscos é conservador, mas internamente ele é desmembrado em métricas por tipologia, de modo que possa ser, posteriormente, medido."*

> *"Trazer com base no teu apetite a risco, conseguir discutir com o tomador de decisão, no sentido de que as decisões fiquem consistentes com esse apetite a risco que foi definido."*

4.1.2. Quais as percepções sobre a gestão de riscos nas organizações públicas?

Para o levantamento deste tópico, foram feitos dois blocos de perguntas. O primeiro teve o objetivo de identificar a opinião do entrevistado sobre o processo de gestão de riscos da sua organização. Para tanto as duas principais perguntas foram: "Qual a sua opinião sobre a gestão de riscos da sua organização"; "Considera que a gestão de riscos subsidia a tomada de decisão?".

A maioria dos entrevistados reconhece que o processo está estabelecido e em funcionamento, mas que necessita de melhorias para conseguir integrar a gestão de riscos à estratégia da organização e subsidiar o gestor na tomada de decisão. Alguns consideram que a gestão de riscos ainda não subsidia a tomada de decisão, mas serve para justificar as escolhas.

> *Então a resposta para você é não, eles não usam para tomar decisão, eles usam para fazer escolhas. Se tem um risco, um controle associado a isso, ele vai e informa; "eu estou comprando isso aqui, porque eu estou executando um controle ali para reduzir um risco". Ou então, "eu estou pedindo para contratar mais funcionário, porque isso aqui é um controle para reduzir um risco".*

Apenas um entrevistado reconheceu que o processo de gestão de riscos da sua organização está integrado com os outros processos e funções organizacionais e apoia a tomada de decisão.

> *"Do ponto de vista de riscos organizacionais, eu diria que, tanto o risco operacional, quanto o risco estratégico, os processos estão estabelecidos e funcionam bem. (...) as três linhas estão bem implementadas e atuam em total sinergia."*
>
> *"Então, toda vez que a [organização] tem uma decisão estratégica para tomar, a diretoria é sempre informada em termos de potenciais impactos, e está olhando qual é o histórico. Então, isso ajuda o tomador de decisão a calibrar a decisão para chegar no ponto certo. Lógico que uma decisão não pode ser, como se diz, tomada única e exclusivamente com base no risco, isso não é o caso, a [organização] tem diversos objetivos, diversos fatores que se referem à decisão, mas a gente acredita e observa pelas evidências que a informação de risco é uma das fundamentais."*
>
> *"Acho que uma das maneiras mais diretas de observar isso é observar a decisão. Ou seja, quando você observa a decisão, e, de novo, essas decisões estão consistentes com o teu apetite declarado, parece que o processo de gestão de risco está funcionando."*

Já o segundo bloco de perguntas, em complemento ao primeiro bloco, teve a finalidade de mapear quais os itens de melhoria os entrevistados identificavam como necessários para a gestão de riscos da sua organização, considerando que a gestão de riscos é um processo contínuo, dinâmico e perene. Os elementos indicados pelos entrevistados estão consolidados no quadro a seguir:

Quadro 12 – Propostas de melhoria para a gestão de riscos organizacional

Propostas de melhoria para o processo atual de gestão de riscos da organização
✓ Avaliar o apetite a risco por tipologia de riscos;
✓ Implementar a decisão baseada em riscos.
✓ Recrutar mais pessoal para a área de riscos
✓ Institucionalizar as metodologias para os riscos estratégicos e tomada de decisão;
✓ Expandir o mapeamento de processos
✓ Implementar teste de estresse dos controles estabelecidos para mitigar o risco

✓ Implementar a gestão de continuidade de negócio.
Melhorias relacionadas ao sistema de TIC
✓ Criar dicionário de causas e consequências; ✓ Construir banco de dados de eventos ✓ Construir banco de dados de mecanismos de controle ✓ Construir banco de dados das consequências ✓ Disponibilizar o catálogo de riscos para os demais órgãos ✓ Documentar os riscos materializados ✓ Desenvolver/atualizar sistema de TIC para a gestão de riscos ✓ Concluir o painel com os riscos estratégicos e para tomada de decisão

Fonte: elaboração própria

Da análise das proposições de melhoria, observa-se que as propostas estavam alinhadas com o estágio de implementação do processo de riscos da organização, havendo um encadeamento lógico e sequencial das etapas de melhoria. Ou seja, quem reivindica mais pessoal, de fato são organizações com as menores equipes; quem indica necessidade de um sistema de TIC, não tem sistema próprio ou o seu sistema não contempla adequadamente as fases do processo de gestão de riscos; quem demanda melhorias nas atividades dos usuários do sistema, como construção de banco de dados, já tem um sistema de TIC estabelecido; e assim por diante.

Por último, em que pese não ser um item de melhoria, falou-se sobre a necessidade de se fazer novo trabalho de sensibilização da alta gestão e sobre o risco de interrupção do processo de implementação da gestão de riscos, tendo em vista que a partir de 1º de janeiro de 2023 haveria troca dos dirigentes dos órgãos, em razão de novo governo.

> *"A sensibilização que a gente fez para alta administração, vai se fazer necessária de novo. É imprescindível, a gente precisa reconquistar, conquistar os novos gestores, os novos líderes. (...) com isso, a gente garante que não vai ter uma grande, digamos assim, uma grande interrupção no processo."*
>
> *"O que precisa ser feito é continuar nesse processo de amadurecimento e, em especial, cuidar para que a rotatividade de gestores que a gente experimenta, que você já falou, que haja uma transferência de conhecimento para eles, de que o fluxo decisório tem que ser feito de uma forma estruturada."*

4.1.3. Quais são os direcionadores para a implementação de uma gestão de riscos bem-sucedida?

Para além de avaliar os aspectos que compõem os processos de gestão de riscos das organizações entrevistadas, pretendeu-se também mapear, a partir da experiência dos entrevistados, quais os fatores que eles consideram essenciais para se implementar uma gestão de riscos eficaz.

Para este levantamento, foram feitas duas perguntas: a primeira "Se fosse implantar uma área de gestão de riscos em uma nova organização como começaria? O que seria prioritário?"; e a segunda "O que considera importante para o sucesso da gestão de riscos dentro de uma organização?". Os fatores apontados pelos entrevistados estão listados na tabela a seguir:

Quadro 13 - Fatores essenciais para uma gestão de riscos eficaz

Como iniciar o processo de implementação?
✓ Mapear os elementos existentes, anteriores à governança
✓ Entender qual o mandato da organização
✓ Definir o sistema de governança
✓ Determinar a unidade executiva
✓ Instituir a Política de Gestão de Riscos
✓ Iniciar pelos riscos operacionais
✓ Iniciar pelos riscos estratégicos
Que fatores são necessários para que a gestão de riscos seja bem-sucedida
✓ Ter apoio e envolver a alta administração
✓ Desenvolver a cultura de riscos
✓ Ter planejamento estratégico
✓ Ter um sistema de TIC adequado para a gestão de risco
✓ Fazer capacitação contínua do corpo funcional
✓ Definir o apetite a riscos
✓ Ter as três linhas de defesa atuando

Fonte: elaboração própria

Para iniciar o processo de gestão de riscos, os entrevistados ressaltaram, como etapas prévias, a importância de entender as demandas da organização, a missão, para

definir como a gestão de riscos pode começar a agregar valor, e o diagnóstico prévio sobre a organização, de modo que essas informações auxiliem no desenho do projeto de implantação da gestão de riscos.

> *"Então, primeiro a gente tem que ter uma fotografia de qual é esse ambiente da organização (...): Se eu tenho mapa de processo; se eu não tenho mapa de processo. Se eu tenho planejamento estratégico; se eu não tenho planejamento estratégico. Se eu tenho análise de ambiente; se em algum momento alguém fez uma análise de ambiente. Qual é o quadro funcional que eu tenho. Terei as pessoas que eu acho que vou conseguir..." (E1-ORG1)*
>
> *"Então, eu acho que é fundamental primeiro, você olhar para a organização e ver qual é o mandato dessa organização. Você tem que ter clareza, o que essa instituição entrega, que produto ela entrega. (...) Eu consigo fazer mais com menos risco?" (E9-ORG2)*
>
> *"Com certeza, a primeira coisa, um assessment dos elementos mais anteriores de governança." (E10-ORG5)*

Já na etapa do desenho do processo de implantação da gestão de riscos, os entrevistados apontaram como relevante o desenho da estrutura de governança, com todos os seus elementos, e não apenas a gestão de riscos como um processo isolado. A institucionalização, a formalização da gestão de riscos por meio da política, foi considerada fundamental, porque é nela que está definido o nível de envolvimento da alta administração, a designação da unidade executiva do processo implantação da gestão de riscos, e o envolvimento e as responsabilidades de todo o corpo funcional da organização.

> *"O desenho de um modelo de governança que englobasse a governança de riscos. A governança geral ter contato com o assunto gestão de riscos." (E3-ORG3)*
>
> *"Eu começaria pela organização e estruturação, pelo sistema de governança. (...) definindo política, competência, atividade, ou seja, eu começaria por ali." (E4-ORG3)*
>
> *"Uma primeira e muito, muito importante, muito relevante é a questão de governança. É uma questão de políticas, definições de atribuições, responsabilidades. Ou seja, cada ente da instituição saber exatamente qual o seu papel dentro de uma estrutura de gerenciamento de riscos." (E9-ORG2)*

Além da importância da regulamentação para a perenidade do processo de gestão de riscos, outro fator apontado foi sobre a existência do modelo das três linhas:

> *"Então, assim, a gente tem que ter, quando a gente fala das três linhas de defesa, é para que independente de quem esteja sentado na diretoria colegiada, a coisa funcione." (E2-ORG1)*

Como elementos essenciais para uma gestão de riscos bem-sucedida, as contribuições foram muito alinhadas entre os entrevistados. O apoio da alta administração foi apontado por 70% dos respondentes como crucial, seguida pela cultura de riscos por mais de 50% dos entrevistados.

> *"É um processo de aprendizado que tem que ser colocado e executado especialmente nos servidores do órgão que lidam com os processos diariamente, porque as chefias vão circular." (E3-ORG3)*
>
> *"Tem que ter momentos de imposição normativa, mas tem que haver também um reconhecimento do custo que isso adiciona e de que é um processo de aprendizado." (E3-ORG3)*
>
> *"Na administração pública, tem que ter cultura porque o nível estratégico muda muito rápido. Se tiver na cultura da organização, o estratégico que chegar para mudar isso vai ter dificuldade porque está na cultura." (E5-ORG3)*
>
> *"Se a alta administração não apoiar, não vou dizer que é impossível, mas você não vai ter lastro." (E8-ORG6)*

Para obter o patrocínio da alta-administração, considerando que é um projeto a ser executado em diversas etapas e a médio e longo prazo, um dos entrevistados destacou como item importante o planejamento adequado deste projeto:

> *É fundamental também pensar em toda essa arquitetura no D0. Ou seja, você não pode estar vendendo para o tomador de decisão só um pedacinho desse desenho. Tem que mostrar a fotografia completa (...). No primeiro ano, vamos avançar um pouco mais na governança. Vamos aprovar a política X, a política Y, a política FX. Quando você faz isso, você ganha tempo, você consegue ir mostrando o resultado, e consegue retroalimentar o processo. E ganhando ali os patrocínios dentro da organização, que são fundamentais para você manter um projeto desse, que é um projeto de longo prazo. (E9-ORG2)*

Outra informação que foi apresentada por alguns dos entrevistados foi referente ao tipo de mapeamento de riscos que priorizaria no seu processo de implantação. Notou-se que a estratégia indicada por eles era compatível com a sua experiência organizacional. Ou seja, a premissa era de um ambiente organizacional semelhante ao que atuava:

> *"Eu não consigo fazer um gerenciamento de risco se eu não tiver o meu planejamento [estratégico], se não tiver estruturado a minha cadeia de valor, meus objetivos, meus valores institucionais." (E4-ORG6)*

> *"Então, a gente começaria pelo estratégico e para ter esse apoio da alta administração e a partir daí passaria para os riscos, para os processos de trabalho." (E6-ORG4)*
>
> *"Mas eu não começaria por risco estratégico, mas nem de projeto, começaria por levantar riscos operacionais. (...) Fazendo gestão de riscos nos processos operacionais, pelo menos os mais críticos, dá para erguer os riscos estratégicos." (E10-ORG5)*

Para complementar o levantamento dos fatores essenciais para a implementação da gestão de riscos, mapeou-se também informações sobre o perfil da equipe considerada adequada pelos entrevistados para trabalhar com a temática de gestão de riscos, quer seja como chefe ou como facilitador.

Muito embora a qualificação técnica e o conhecimento do negócio da organização tenham sido apontados por muitos como relevantes, foi unânime a referência pelos entrevistados à importância das habilidades e competências interpessoais (os chamados *soft skill*) para os servidores que atuam nas funções da segunda linha.

> *"Tem que ter relacionamento interpessoal, não tem jeito. Tem que conseguir tratar com as pessoas porque em algum momento você vai precisar convencer as pessoas que elas precisam fazer algo que elas não fazem ainda." (E1-ORG1)*
>
> *"Então, eu acho que na verdade é muito mais naquela linha de alguns soft skills que são necessários para tocar bem essa temática, porque para fechar porta esse tema é ótimo. Dependendo da sua abordagem, você fecha um monte de porta, você não sai do outro lado, está emparedado." (E6-ORG4)*
>
> *"Tem que ter pessoas, isso já virou meio clichê, mas tem que ter soft skills, de entender que o cara vai te xingar no começo, aí tem que ter resiliência. (...) ser meticuloso, crítico, pessoas que questionam." (E8-ORG6)*
>
> *"Também tem que ter um ferramental quantitativo, lógico, você acaba mexendo com isso também, mas soft skills também são muito importantes nesse grupo de pessoas. E de novo, vão estar interagindo com a organização inteira, mediando conflitos, mediando discussões." (E9-ORG2)*
>
> *"Eu não acredito muito em área de risco muito inchada, muita gente. Menor quantidade de gente, mas gente que realmente tem interesse em avançar, em termos de conhecimento e qualificação." (E9-ORG2)*

4.1.4. Como a auditoria interna pode ajudar a projetar, desenvolver e implementar políticas e práticas de gestão de riscos no setor público?

Observado o modelo de auditoria interna governamental para as organizações públicas do Poder Executivo federal, as organizações integrantes da administração indireta (ORG1, ORG2 e ORG5) possuem unidades de auditoria interna própria (Audin), ao passo que a Controladoria-Geral da União (CGU) é a unidade de auditoria governamental para os ministérios (ORG3 e ORG4). Além disso, cabe à CGU, como órgão central do Sistema de Controle Interno, a orientação normativa e supervisão técnica às UAIGs, assim como estabelecer diretrizes quanto à realização de ações integradas pelas UAIGs (BRASIL, 2001, 2017a).

Nesse contexto, as perguntas foram divididas para avaliar dois cenários: primeiro, a relação existente entre a área de riscos e a unidade de auditoria interna governamental da organização – Audin ou CGU, a depender da organização; e segundo, a relação da organização com a CGU no exercício das competências previstas na IN 01, de 2016, e demais normativos que se seguiram, na temática gestão de riscos organizacionais.

O resultado do levantamento da relação existente entre a área de riscos e a unidade de auditoria interna governamental está representado no quadro a seguir:

Quadro 14 – Formas de atuação da AI na GR da organização

De que forma a Auditoria Interna contribui para GR da organização??
✓ Utiliza as informações da gestão de riscos para o planejamento das auditorias baseadas em riscos. ✓ Participa do Comitê de Governança ✓ Participa das discussões dos indicadores de riscos ✓ Audita processos que a organização precisa mesmo desenvolver ✓ Emite recomendações que ajudam a gestão de riscos da organização.

Fonte: elaboração própria

Para os entrevistados, as recomendações feitas para a melhoria do processo de gestão de riscos e a participação da auditoria no comitê de governança aumentam a

relevância da temática gestão de riscos na organização e empoderam o papel da área de riscos juntos às unidades internas da entidade.

> *Quando a área não tem avaliação de riscos do processo a ser auditado, a auditoria interna emite a recomendação de que se faça a avaliação de risco. (E1-ORG1)*
>
> *As recomendações ajudam a área de riscos na implementação de um plano de continuidade, ou na mitigação de algum risco que a área de riscos também entendeu que ficou um pouco fora do apetite da organização. (E9-ORG2)*
>
> *A auditoria participa também do GRC e acaba reforçando alguma preocupação, alguma prioridade que o tomador de decisão tem que estar observando. (E9-ORG2)*
>
> *Então é útil, porque ele te empurra para frente, através das solicitações de auditoria, através das recomendações de auditoria. (E10-ORG5)*

No tocante à auditoria baseada em riscos, foi unânime entre os entrevistados a opinião de que a auditoria interna se vale das informações produzidas pela área de riscos para subsidiar o planejamento das auditorias da organização. E como consequência disso, a percepção dos entrevistados é de que as auditorias são em áreas mais críticas e produzem informações úteis para a organização.

> *Quando eles estão vindo auditar políticas públicas, eles estão fazendo auditoria operacional baseada em riscos, eles se valem dos riscos. Tem esse relacionamento e a gente contribui para melhorar esse documento dos eventos de risco deles, da própria CGU. (E4-ORG3)*
>
> *Eles precisavam levantar os objetos auditáveis, conforme a priorização de lá e a ideia deles era garantir que os trabalhos de fato passassem a agregar mais valor à gestão aqui do Ministério. O foco era nos objetos mais relevantes, o trabalho deles foi partir de uma visão de quem está olhando de fora, pra tentar harmonizar esse plano de auditoria interna baseado em risco com o plano estratégico nosso aqui do Ministério. (E6-ORG4)*
>
> *Igual eu falei lá, as auditorias deles, eles são cuidadosos para auditar assuntos que a gente está precisando mesmo se desenvolver. (...) Eles vão vendo a gente e aí eles apontam, "ó, sua matriz de calor não está legal", igual apontaram agora. "Você precisa diminuir a quantidade de probabilidade de impacto de risco médio, isso aí tem que ser, tem que aumentar". (E10-ORG5)*

Para mapear o segundo cenário, duas perguntas foram feitas: a primeira, se a CGU atuou de alguma forma no processo de implantação da gestão de riscos da organização; a

segunda, de que forma o entrevistado avalia que a CGU pode contribuir para o processo de gestão de riscos das organizações. A síntese dos fatores elencados pelos respondentes consta no Quadro 15:

Quadro 15 – Formas de atuação da CGU na GR da organização

A CGU participou do processo de implantação da GR?
✓ Fez capacitação dos servidores da organização ✓ Houve cobrança da CGU a respeito da implantação da gestão de riscos na organização
De que forma a CGU pode atuar no processo de GR da organização?
✓ Avaliar a gestão de riscos dos órgãos que já possuem o processo estabelecido ✓ Dar consultoria aos órgãos que estão com dificuldade em implantar o seu processo de gestão de riscos ✓ Disponibilizar um catálogo de riscos ✓ Emitir recomendações que ajudem no patrocínio interno

Fonte: elaboração própria

Na avaliação dos entrevistados a CGU pode contribuir de diversas formas para a melhoria do processo de gestão de riscos da organização, conforme sugestões apresentadas no quadro acima, e, por meio das suas recomendações, pode promover melhorias no processo e ajudar no patrocínio interno da área de riscos.

> *A atuação da CGU é um trampolim positivo para se fazer melhoria e inclusive pressionar para se conseguir aquilo que é preciso para o trabalho. (E2-ORG1)*
>
> *Eu considero que se não houvesse o envolvimento da CGU, a gestão de risco não teria sido implementada com a mesma velocidade e intensidade como ela foi. (E3-ORG3)*
>
> *Do ponto de vista de fazer todo o processo de gestão de riscos funcionar, é fundamental a atuação da CGU. Primeiro, porque dá uma visão externa do que a área de riscos está fazendo. Segundo, ajuda para o patrocínio interno, no sentido de promover mudanças, de avançar. (E9-ORG2)*

4.2. Discussão dos Resultados

(Yin, 2010) descreve cinco técnicas de análise de estudos de dados: 1) combinação de padrão; 2) construção de explanação; 3) análise de séries temporais; 4) modelos lógicos;

e 5) síntese cruzada de casos. Dada a natureza das questões abordadas e do objetivo pretendido pela pesquisa, a combinação de padrões e a síntese cruzada de casos apresentam-se como as formas de análise mais adequadas, uma vez que o primeiro consiste na identificação de determinados padrões no caso de estudo e a sua comparação com os previstos teoricamente e o segundo permite comparar as similaridades e diferenças entre os casos.

Embora a qualidade da análise dependa da estratégia ou técnica usada para a análise dos dados, a qualidade dos resultados depende ainda das seguintes premissas para a análise: 1) deve considerar todas as evidências; 2) se possível, deve considerar todas as interpretações rivais importantes; 3) deve abordar os aspectos mais significativos do estudo de caso; e 4) deve-se considerar o conhecimento prévio de especialista do investigador no estudo de caso (Yin, 2010).

4.2.1. Como as organizações públicas implementam as práticas de gestão de riscos?

Das seis organizações pesquisadas, duas institucionalizaram a sua gestão de riscos anterior à regulamentação da gestão de riscos na administração pública federal, as outras quatro só tiveram a sua política de gestão de riscos a partir de 2016. Em seu levantamento, o TCU observou que os avanços da implementação da gestão de riscos na administração pública federal só foram significativos após a regulamentação do tema (BRASIL, 2021).

Estes avanços podem ser explicados segundo o que defende (Woods, 2009) de que a política do governo central orienta muitos dos objetivos estratégicos e determina os recursos disponíveis das organizações. Ou seja, a normatização federal influencia implicitamente as organizações a investir em sistemas de gestão de riscos, por conseguinte, pode indicar melhora no nível de maturidade dessas organizações.

As estratégias utilizadas pelas organizações para iniciar o processo de implantação da gestão de riscos foram diversas, o que era de se esperar em razão do seu grau de autonomia administrativa, da sua natureza jurídica, da capacidade orçamentária e financeira, do tamanho da sua força de trabalho, dentre outros fatores.

Nas organizações da administração indireta, por regra, os seus dirigentes têm mandatos e a estrutura de governança da organização, como diretoria colegiada, conselho de administração, comitê de auditoria, etc., já estava estabelecida antes mesmo da regulamentação da gestão de riscos na administração pública federal.

Por outro lado, nas organizações da administração direta, por não terem essa estrutura de governança já estabelecida, a implementação da gestão de riscos ocorreu em outra dinâmica. Houve o trabalho prévio de estruturar e institucionalizar um sistema de governança *"que englobasse a governança de riscos" (E3)*. Nos ministérios, não existia a cultura de decisões em colegiado ou dos dirigentes divulgarem entre si os riscos das suas políticas, programas e projetos. Havia, portanto, o grande o desafio de mostrar que esta nova forma de dirigir uma organização era mais eficiente e permitia tomar melhores decisões, com menos riscos.

A questão importante era que os ministros precisavam estar envolvidos nos processos de gestão de risco como parte da boa governança (Barrett AO, 2014) e esta consciência ainda não existia. Isso pode ser explicado porque a governança e a cultura de gestão de riscos são a base dos demais componentes de gestão de riscos na organização (COSO, 2017; IBGC, 2017).

Na nossa pesquisa, observou-se que coube aos Assessores Especiais de Controle Interno (AECI) promover esse trabalho de convencimento, envolvimento e engajamento da alta administração, com o suporte da CGU que, naquele momento, por meio do trabalho de auditoria, recomendava a implantação da gestão de riscos em processos e políticas públicas mais sensíveis.

A atuação dos AECIs para estruturar o sistema de governança e angariar o apoio da alta administração demandou muita resiliência, uma vez que a troca de dirigentes (ministros e secretários) entre o período de 2017 a 2022 foi recorrente para algumas pastas ministeriais.

> *É em 2017, como eu falei, (...) estou aqui até hoje. Eu passei com (...), acho que deve ser o sétimo ministro.*
>
> *Tivemos diversos ministros em pouco tempo. Quando a gente acabava de convencer da questão da importância do planejamento estratégico, aí vinha outro ministro.*

A atuação da AECI no processo de implantação da gestão de riscos foi considerada fundamental pelo entrevistado da alta gestão do ministério:

> *Eu avalio como fundamental, porque a gente tem duas dimensões nesse processo, a gente tem a interferência do pessoal do planejamento e a interferência do pessoal do controle. (...) Quando o controle interno se envolve, a sensação do gestor é diferente, a sensação do gestor é que ele está tendo uma validação para o curso decisório que ele está tomando, e uma situação que alivia o temor de tomar a decisão errada.*
>
> *Foi muito feliz a escolha do Ministério em colocar o controle de riscos associado com o controle interno, até porque isso dá muita ferramenta para o controle interno desenvolver o que a gente costumou chamar de atuação preventiva. Então, dá segurança, tem um efeito psicológico interessante para o gestor, que ele se sente apoiado pelo controle interno e validado, de certa forma, na decisão que ele toma.*

A atuação da CGU neste processo de institucionalização foi também destacada pelo integrante da alta gestão:

> *houve a cobrança da CGU a respeito da implantação desses mecanismos (...). Eu considero que se não houvesse o envolvimento da CGU, a gestão de risco não teria sido implementada com a mesma velocidade e intensidade como ela foi.*

O protagonismo da atuação da AECI no processo de institucionalização da gestão de riscos foi também percebido por (Vanderlei, 2022) em seu estudo de caso. Para ele, a AECI foi responsável por decisões e ações que permitiram o desenvolvimento do processo de gestão de riscos da organização, mesmo diante das diversas adversidades que surgiram ao longo dos seis anos.

Como estratégia para angariar o apoio da alta administração, neste ambiente político instável, as AECIs iniciaram a implantação pelos riscos estratégicos. Dessa forma elas conseguiriam apresentar resultados “rápidos” às instâncias de governança do órgão e demonstrar os ganhos da gestão de riscos. Considerando que os riscos estratégicos eram em menor número, se comparados com os riscos de processo, gerenciá-los por meio de planilhas seria mais simples, menos trabalhoso, e mais rápido de mapeá-los.

No ambiente das organizações pesquisadas, os sistemas de TIC não se mostraram essenciais para iniciar a implementação da gestão de riscos, mas à medida que a organização aumentava os seus processos mapeados ou avançava para as etapas de

monitoramento e comunicação dos riscos, a ferramenta mostrou-se fundamental. Nas duas organizações onde não há um sistema de TIC ou o sistema não é adequado para a gestão de riscos, os entrevistados relataram muitas dificuldades em expandir o mapeamento de riscos para mais processos, em monitorar a implementação do plano de tratamento, em produzir informações gerenciais para os gestores de riscos, dentre outras medidas. Essa evidência está alinhada às descobertas de (Woods, 2009) de que inadequações ou limitações no fornecimento de TIC podem prejudicar o acesso a informações de risco e a operação efetiva do sistema de gestão de riscos.

A presença de representantes de risco nomeados por cada diretoria para implementar uma abordagem prática e viável para a gestão de risco dentro de sua diretoria também foi um recurso mapeado por (Woods, 2009) em seu estudo de caso. Para além de reforçar as atividades de monitoramento e supervisão da segunda linha, observou-se que o uso dos agentes de riscos e dos comitês gerenciais e táticos contribuía para o desenvolvimento da cultura de riscos da organização, uma vez que permitia o envolvimento de funcionários em diferentes posições hieráquicas, com diferentes níveis de responsabilidades (Mahama et al., 2022).

As organizações com maiores orçamentos e força de trabalho também foram as que apresentaram as melhores estruturas de recursos humanos e tecnológicas para gerenciar os seus riscos organizacionais. Nessas organizações notou-se também maior integração da gestão de riscos à estratégia e aos processos da organização, inclusive integração a nível de sistema de TIC. Este resultado é compatível com as descobertas de (Woods, 2009) de que grandes organizações usam sistemas formais de gestão de riscos, gerenciados por especialistas que fazem uso de tecnologias sofisticadas relevantes.

No que se refere às características das unidades da área de gestão de riscos, notou-se que havia correspondência entre o tamanho da força de trabalho da organização e o tamanho das equipes das áreas de riscos. No geral, são unidades pequenas e coesas, com integrantes oriundos de áreas diversas da organização, o que contribui para uma melhor interlocução entre a área de riscos e as demais unidades da organização.

Em síntese, observou-se que os princípios de gestão de risco estão sendo integrados nos processos globais de gestão e governança das organizações pesquisadas,

mas em níveis diferentes. Alguns dos recursos utilizados para promover essa integração e o aculturamento nas organizações estudadas, são:

- Atuação dos comitês táticos e gerenciais de gestão de riscos;
- Monitoramento permanente dos indicadores chaves de riscos;
- Comunicação periódica às instâncias de governança;
- Integração da gestão de riscos à estratégia da organização;
- Participação da auditoria interna no comitê de governança;
- Abordagem da auditoria baseada em riscos pela auditoria interna;
- Software integrado de gestão de riscos;
- Capacitação contínua dos agentes e gestores de riscos;
- Comunicação permanente com os servidores e funcionários da instituição;

4.2.2. Quais as percepções sobre a gestão de riscos nas organizações públicas?

A gestão de riscos contribui para uma mudança de foco de conformidade legalista para o de responsabilidade que enfatiza a medição de desempenho e a formulação de estratégias (Rana, Hoque, et al., 2019). Contudo, se não houver integração entre a gestão de riscos e os demais processos de gestão da organização, a gestão de riscos pode se transformar em um processo formal e padronizado sem considerar o contexto organizacional e seus requisitos. Ele existirá apenas para cumprir com os requisitos de conformidade e regulatórios (Bracci et al., 2022).

Embora haja a necessidade de integrar a gestão de riscos aos processos de negócios das organizações públicas, há poucas evidências de que isso tenha sido feito na prática (Bracci et al., 2022).

Apenas um dos entrevistados reconheceu que o processo de gestão de riscos da sua organização está integrado com os outros processos e funções organizacionais e apoia a tomada de decisão. Os demais entrevistados reconhecem que o processo está estabelecido e em funcionamento, mas que necessita de melhorias para conseguir integrar a gestão de riscos à estratégia da organização e subsidiar de fato o gestor na tomada de decisão.

Após mais de seis anos, o nível de implementação da gestão de riscos nas organizações públicas ainda é muito variável. Esses resultados estão em linha com as preocupações apontadas por (Rana, Hoque, et al., 2019; Vieira & Araújo, 2020) de que é necessário adotar uma perspectiva de longo prazo nas organizações do setor público para que sistemas consistentes de gestão de riscos possam ser efetivamente implementados. E esse trabalho pode levar muitos anos para produzir seu impacto, devendo as reformas no desempenho e na avaliação de risco serem contínuas, em vez de refletir apenas um foco de curto prazo ou de prazo fixo(Rana, Hoque, et al., 2019).

4.2.3. Quais são os direcionadores para a implementação de uma gestão de riscos bem-sucedida?

Considerando que o apoio da alta administração foi apontado por 7 (sete) dos 10 (dez) respondentes, seguido pela cultura de riscos pela metade dos entrevistados como elementos essenciais para se implementar a gestão de riscos, o ambiente mais favorável está nas organizações da administração indireta com dirigentes com mandatos fixos e estrutura de governança estabelecida. Isto pode justificar, por exemplo, o maior número de entidades da administração indireta com o nível de maturidade aprimorado 78, se comparado com a quantidade de 11 (onze) órgãos da administração direta (BRASIL, 2021).

Nas organizações em que o ambiente político é instável e a alta gestão muda constantemente, é necessário cuidar para que a estrutura de governança não se enfraqueça e o processo de gestão de risco não se interrompa ou não retroceda. Os resultados apontam que, apesar dos sistemas de gestão de riscos definidos pelos ministérios estarem inseridos nas estruturas de governança, na maioria dos casos, a implementação destes sistemas tem sido sistematicamente interrompida (Vieira & Araújo, 2020).

Para mitigar esses riscos, é preciso desenvolver mecanismos de proteção. Alguns dos entrevistados apontaram a necessidade de se trabalhar a cultura de riscos da organização pública:

> *O estratégico muda constantemente, mas os servidores que lidam com os processos diariamente permanecem.*

> *Se tiver na cultura da organização, o estratégico que chegar para mudar isso vai ter dificuldade porque está na cultura.*

À exceção da divergência entre a estratégia de iniciar ou não a gestão de riscos pelos riscos estratégicos ou operacionais, a identificação dos fatores essenciais para implementar a gestão de riscos estava alinhada entre os entrevistados, independentemente das características do seu ambiente organizacional. O foco principal foi em estruturar o sistema de governança, instituir a política de riscos e garantir o apoio da alta administração para possibilitar desenvolver a cultura de riscos. Essas contribuições reforçam as conclusões de (Abidin, 2017; Castanheira et al., 2010; Selim & McNamee, 1999a) de que um ambiente de risco mais formalizado promove a existência de uma forte cultura de consciência de risco.

4.2.4. Como a auditoria interna pode ajudar a projetar, desenvolver e implementar políticas e práticas de gestão de riscos no setor público?

Para os entrevistados a atuação da auditoria interna contribui diretamente para o desenvolvimento da cultura de riscos, especialmente quando participa das discussões no comitê de governança e quando aplica a abordagem de riscos nas auditorias. A participação do auditor-chefe nas discussões de risco organizacional com outros gestores seniores foi apontada por (Selim & McNamee, 1999b) como um fator-chave na gestão eficaz dos riscos e para a auditoria interna.

Para a aplicação da auditoria baseada em riscos, o auditor se vale das informações produzidas pela área de riscos para subsidiar o planejamento das auditorias da organização. O reflexo disso, na percepção dos entrevistados, é de que as auditorias são em áreas mais críticas e produzem informações úteis para a organização. Isso pode ser explicado, porque a auditoria baseada em risco aumenta a capacidade da auditoria interna em garantir que os riscos potenciais que impedem o alcance dos objetivos da empresa sejam mitigados adequadamente (Abidin, 2017; Audit Commission, 2001; Castanheira et al., 2010; Selim & McNamee, 1999b). A atuação da auditoria interna nos processos de

gestão de riscos tem como objetivo aumentar o valor agregado da auditoria às necessidades específicas das organizações (Arena & Azzone, 2009a).

Para além da aplicação da auditoria baseada em riscos em seus trabalhos, os entrevistados ressaltaram a importância da CGU em avaliar a gestão de riscos dos órgãos que já possuem o processo estabelecido e dar consultoria aos órgãos que estão com dificuldade em implantar o seu processo de gestão de riscos.

Em que pese essas demandas estarem em linha com as competências previstas para as funções de uma unidade de auditoria interna (Arena & Azzone, 2009b; BRASIL, 2017a, 2018b; Castanheira et al., 2010; IIA, 2017, 2020; Selim & McNamee, 1999a, 1999b), os entrevistados identificaram a CGU, possivelmente por não compor a estrutura do órgão, como mais adequada para prestar os serviços de consultoria e avaliação dos processos de governança, gestão de riscos e controles internos da organização.

> *Ou seja, qual o papel de um TCU, de uma CGU, quando chega e tem uma auditoria externa em uma organização pública? Eu diria que é fundamental. (...). Às vezes, e faz parte da natureza de um órgão público, nem sempre é fácil avançar com mudanças. Então, quando vem alguém de fora, com um olhar externo, que identifica caminhos que você possa melhorar, eu acho que isso também ajuda em termos de patrocínio e para que as coisas avancem.*

> *Assim, a CGU deveria operar como se ela fosse uma auditoria externa, tá? Ela vai auditar o processo de avaliação de riscos dos órgãos. (...) quem tem dificuldades, não tem como implementar ou não está conseguindo implementar, ela vai lá e sugere o modelo dela.*

A OCDE destacou o papel central da CGU no apoio e indução da implementação de sistemas de gestão de riscos nos órgãos da administração pública federal, mas, por outro lado, ressaltou a necessidade de uma liderança comprometida com a criação de uma cultura de gestão que promova a gestão de riscos como ferramenta estratégica do sistema de governança (BRASIL, 2018b; OECD, 2012).

A partir dos novos marcos regulatórios sobre governança e gestão de riscos, a CGU incorporou novas competências regimentais, mas ainda assim não havia definição quanto à responsabilidade institucional pela temática gestão de riscos na administração pública do Poder Executivo federal. Para um dos entrevistados, esta indefinição legal repercute, por

exemplo, no desenvolvimento, implantação e manutenção de uma ferramenta tecnológica para apoiar a gestão de riscos organizacionais, ou na estruturação de unidade de apoio técnico sobre gestão de riscos, o que demanda recursos financeiros e desenvolvimento de novas competências, dentre outras medidas.

Espera-se que esta lacuna tenha sido suprida por meio do Decreto nº 11.330, de 2023, em que estabeleceu à CGU o suporte à gestão de riscos como uma área de sua competência.

5. CAPÍTULO IV - CONCLUSÃO

Entre os diferentes mecanismos de governança pública, a gestão de riscos, no contexto brasileiro, ganhou nos últimos seis anos grande atenção devido às suas ligações com o sistema de controles internos da gestão. Por ser um tema recente, o presente estudo objetiva preencher uma lacuna de conhecimento sobre os principais fatores impulsionadores e inibidores do processo de institucionalização da gestão de riscos organizacionais do setor público brasileiro.

Para identificar esses principais direcionadores, o estudo foi segmentado em quatro grandes tópicos. O primeiro deles foi identificar como as organizações públicas implementaram o seu processo de gestão de riscos. O segundo foi mapear a opinião do entrevistado sobre a gestão de riscos da sua organização. O terceiro, mapear os principais direcionadores para iniciar a implementação da gestão de riscos em uma organização pública. E, por último, identificar, sob a perspectiva da organização, se a auditoria interna atuou e de que forma na gestão de riscos da organização.

Considerando a recolha dos dados por meio de entrevistas semiestruturadas a nove entrevistados de seis organizações públicas, os resultados revelaram que os fatores essenciais para implementar a gestão de riscos organizacional são: o sistema de governança; a política de riscos; e o apoio da alta administração.

No entanto, notou-se que a existência e a consistência desses elementos dependem das características organizacionais, como, por exemplo, como é constituída a alta gestão (com ou sem mandato), o grau de autonomia administrativa, a natureza jurídica, a capacidade orçamentária e financeira, a composição da sua força de trabalho, dentre outros fatores.

As organizações da administração direta, por não terem uma estrutura de governança já estabelecida para a implementação da gestão de riscos, demandaram o trabalho prévio de estruturar e institucionalizar todo o seu sistema de governança. Nas organizações onde não havia essa estrutura de governança estabelecida, o ambiente político era instável e a alta gestão mudava constantemente (ministérios), a atuação ativa do Assessor Especial de Controle Interno (AECI) mostrou-se imprescindível para garantir o apoio da alta administração, estabelecer o modelo de governança e desenvolver a cultura

de riscos. A opção de iniciar a implantação pelos riscos estratégicos foi justificada como estratégia encontrada para apresentar resultados “rápidos” às instâncias de governança do órgão e, assim, obter o apoio e engajamento da alta administração.

As organizações da administração indireta, por outro lado, apresentaram um ambiente mais favorável para implementar a gestão de riscos, porque a estrutura de governança da organização já estava estabelecida e havia estabilidade dos seus dirigentes. Assim, o apoio da alta administração (*tone at the top*) se manteve e, por conseguinte, a cultura de riscos se desenvolveu gradualmente à medida que a gestão de riscos apresentou benefícios à tomada de decisão e ao alcance dos objetivos organizacionais.

O sistema de TIC não se mostrou essencial para iniciar a implementação da gestão de riscos, mas, à medida que a organização avançava em seus processos mapeados ou nas etapas de monitoramento e comunicação dos riscos, a ferramenta mostrou-se fundamental. Todas as propostas de melhoria das organizações pesquisadas estavam relacionadas com o sistema de TIC de forma direta ou indireta.

No geral, os resultados revelaram que os princípios da gestão de risco estão sendo integrados nos processos globais de gestão e governança das organizações pesquisadas, mas em níveis diferentes, o que justifica a maioria dos entrevistados reconhecerem que a gestão de riscos da sua organização ainda não consegue subsidiar a tomada de decisão.

Independentemente do ambiente organizacional, os entrevistados destacaram que a atuação da auditoria interna governamental (Audin e CGU) contribuiu substancialmente para o desenvolvimento da cultura de riscos da organização, especialmente quando a auditoria interna participa das discussões no comitê de governança, quando aplica a abordagem de riscos nas auditorias e quando faz recomendações que impulsionam melhorias no processo de gestão de riscos da organização. Adicionalmente, notou-se uma expectativa maior em relação à CGU em prestar os serviços de consultoria e avaliação dos processos de gestão de riscos da organização.

Os resultados revelaram ainda que não existe uma única forma para implementar um modelo de gestão de riscos organizacional no setor público, nem uma única estrutura adequada, uma vez que o contexto organizacional tem influência direta.

Decorridos pouco mais de seis anos de 'institucionalização' da gestão de riscos organizacional nas entidades públicas do governo federal, é preciso aceitar que, para que a gestão de riscos não seja apenas uma prática burocrática ou exista apenas para cumprir um requisito regulatório, este processo de integração e de suporte à tomada de decisão pode levar muitos anos e precisa de uma liderança governamental.

Ao responder as questões de pesquisa, com o registro das experiências e das lições aprendidas pelas organizações estudadas, esta investigação pode servir de referência para outras organizações do setor público no seu processo de implementação da gestão de riscos organizacional; fomentar o intercâmbio de experiências das práticas de gestão de riscos entre as organizações públicas; e subsidiar, de alguma forma, o planejamento das estratégias de atuação das auditorias internas governamental e da Controladoria-Geral da União, especialmente nas atribuições regimentais relacionadas à gestão de riscos, atualizadas pelo Decreto nº 11.330, de 2023; e, por fim, abrir novos campos de pesquisa nesta área de gestão.

As conclusões do presente estudo apresentam pelo menos as seguintes limitações. A primeira é decorrente da utilização de uma abordagem qualitativa para a recolha de dados, na qual os resultados são limitados em termos da sua generalidade. Os dados recolhidos representam as percepções individuais dos entrevistados e, portanto, podem não ser representativos ou generalizáveis para as demais organizações da administração pública federal. No entanto, dado que o presente estudo teve por objetivo fornecer profundidade, a utilização de entrevistas semi-estruturadas foi considerada adequada para cumprir este objetivo.

A segunda limitação está no viés potencial de seleção da amostra, uma vez que os entrevistados foram selecionados a partir da facilidade de acesso da entrevistadora às potenciais organizações. Adicionalmente, consideraram-se apenas organizações com sistemas de gestão de riscos aprimorados.

Em futuras pesquisas seria interessante alagar o âmbito a organizações em fases mais primárias de implementação de sistemas de gestão de riscos. Além disso, considerando os diversos modelos de estruturas organizacionais, mais pesquisas precisam ser realizadas para obter um resultado mais robusto - um *framework* de boas práticas para a implementação de uma gestão de riscos integrada no setor público.

6. Referências Bibliográficas

Abidin, N. H. Z. (2017). Factors influencing the implementation of risk-based auditing. *Asian Review of Accounting*, *25*(3), 361–375. https://doi.org/10.1108/ARA-10-2016-0118

Arena, M., & Azzone, G. (2009a). Identifying Organizational Drivers of Internal Audit Effectiveness. *International Journal of Auditing*, *13*(1), 43–60. https://doi.org/10.1111/j.1099-1123.2008.00392.x

Arena, M., & Azzone, G. (2009b). Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing*, *13*(1), 43–60.

Audit Commission. (2001). *Worth the risk: improving risk management in local government*. Audit Commission Publications.

BARDIN, L. (2013). *Análise de Conteúdo* (Edições 70).

Barrett AO, P. (2014). New development: Risk management - how to regain trust and confidence in government. *Public Money & Management*, *34*(6), 459–464. https://doi.org/10.1080/09540962.2014.962376

BID. (2018). *Better spending for better lives: how Latin America and the Caribbean can do more with less* (A. Izquierdo, C. Pessino, & G. Vuletin, Eds.). Washington, D.C: Inter-American Development Bank. https://doi.org/10.18235/0001217-en

Bracci, E., Mouhcine, T., Rana, T., & Wickramasinghe, D. (2022). Risk management and management accounting control systems in public sector organizations: a systematic literature review. *Public Money & Management*, *42*(6), 395–402.

BRASIL. (2001). *Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 10.180, de 6 de fevereiro de 2001. Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências.* Retrieved from http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10180.htm

BRASIL. (2016). Presidência da República. Controladoria-Geral da União. Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos,

gestão de riscos e governança no âmbito do Poder Executivo federal. In *Diário Oficial da União, Brasília, ed. 89, s. 1, p. 14, 11 maio 2016*. Retrieved from https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&data=11/05/2016&pagina=14

BRASIL. (2017a). *Controladoria-Geral da União. Secretaria Federal de Controle Interno. Instrução Normativa nº 3, de 9 de junho de 2017. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal*.

BRASIL. (2017b). Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. In *Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos* (No. 9.203). BRASIL: Diário Oficial da União, Brasília, s. 1, p. 3, 23/11/2017.

BRASIL. (2018a). *Tribunal de Contas da União. Referencial básico de gestão de riscos*. Brasília: Secretaria Geral de Controle Externo (Segecex).

BRASIL. (2018b). *Tribunal de Contas da União. Roteiro de Avaliação de Maturidade da Gestão de Riscos*. Brasília: Secretaria de Métodos e Suporte ao Controle Externo.

BRASIL. (2020a). *Tribunal de Contas da União. Manual de Gestão de Riscos do TCU* (2nd ed.). Brasília: Secretaria de Planejamento, Governança e Gestão (Seplan).

BRASIL. (2020b). *Tribunal de Contas da União. Referencial Básico de Governança Organizacional* (3rd ed.; TCU, Ed.). Brasília: Secretaria de Controle Externo da Administração do Estado – SecexAdministração.

BRASIL. (2021). *Tribunal de Contas da União. Perfil Integrado de Governança Organizacional e Gestão Públicas – 2021*. Retrieved from https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E7BE7E47C017C0DA388291F10

BRASIL, & Controladoria Geral da União. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. , Diário Oficial da União, Brasília, s. 1, p. 3, 23/11/2017 § (2017).

Castanheira, N., Rodrigues, L. L., & Craig, R. (2010). Factors associated with the adoption of risk-based internal auditing. *Managerial Auditing Journal*, *25*(1), 79–98. https://doi.org/10.1108/02686901011007315

Cavalcante, P. L. C., & Pires, R. R. C. (2018). *Governança pública: das prescrições formais à construção de uma perspectiva estratégica para a ação governamental*.

CGU. (2017). *Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo federal*. Brasília: Secretaria Federal de Controle Interno. Retrieved from https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-1.pdf

COSO. (2004). *Gerenciamento de Riscos Corporativos - Estrutura Integrada*.

COSO. (2013). *Controle Interno - Estrutura Integrada*.

COSO. (2017). *Gerenciamento de Riscos Corporativos: Integrado com Estratégia e Performance* (IIA Brasil e PWC). São Paulo: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Dias, A. A. de S. P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000: 2009? *Revista Perspectiva Empresarial*, *4*(2), 73–82. Retrieved from https://revistas.ceipa.edu.co/index.php/perspectiva-empresarial/article/view/134

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance*, *82*(3), 625–657. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1111/jori.12035

Hutchins, G. (2018). *ISO 31000: 2018 enterprise risk management*. Greg Hutchins. Retrieved from https://books.google.pt/books?hl=en&lr=&id=csx7DwAAQBAJ&oi=fnd&pg=PT5&dq=iso+31000+2018&ots=W9OjAJSlaO&sig=OHENzNxSR0pGVWUBr4TV9DxGaZA&redir_esc=y#v=onepage&q=iso%2031000%202018&f=false

IBGC. (2017). *Gerenciamento de riscos corporativos: evolução em governança e estratégia*. São Paulo, SP: Instituto Brasileiro de Governança Corporativa (Série Cadernos de Governança Corporativa, 19). Retrieved from www.ibgc.org.br

IIA. (2017). *Norma de Implantação 2120: Gerenciamento de Riscos*. Retrieved from https://iiabrasil.org.br/korbilload/upl/ippf/downloads/2019orientacoes-ippf-00000013-07042020104945.pdf

IIA. (2020). *Modelo das Três Linhas do IIA 2020*.

ISO. (2018). *INTERNATIONAL STANDARD ISO 31000:2018(E). Risk management - Guidelines*.

Mahama, H., Elbashir, M., Sutton, S., & Arnold, V. (2022). Enabling enterprise risk management maturity in public sector organizations. *Public Money & Management*, *42*(6), 403–407.

Nogueira, R. A., & Gaetani, F. (2018). *A questão do controle no debate de governança pública*.

OECD. (2012). *OECD Integrity Review of Brazil*. OECD Publishing. https://doi.org/10.1787/9789264119321-en

OECD. (2020). *Panorama das Administrações Públicas: América Latina e Caribe 2020*. OECD. https://doi.org/10.1787/9e6d37a1-pt

Power, M. (2007). *Organized Uncertainty : Designing a World of Risk Management*. Oxford: OUP Oxford. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=201112&lang=pt-pt&site=ehost-live&scope=site

Prewett, K., & Terry, A. (2018). COSO's updated enterprise risk management framework—A quest for depth and clarity. *Journal of Corporate Accounting & Finance*, *29*(3), 16–23. Retrieved from https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=69fec63b-6962-43d2-bf87-925a493a4eb2%40redis

Rana, T., Hoque, Z., & Jacobs, K. (2019). Public sector reform implications for performance measurement and risk management practice: insights from Australia. *Public Money & Management*, *39*(1), 37–45.

Rana, T., Wickramasinghe, D., & Bracci, E. (2019). New development: Integrating risk management in management control systems—lessons for public sector managers. *Public Money & Management*, *39*(2), 148–151.

Selim, G., & McNamee, D. (1999a). Risk Management and Internal Auditing: What are the Essential Building Blocks for a Successful Paradigm Change? *International Journal of Auditing*, *3*(2), 147–155. https://doi.org/10.1111/1099-1123.00055

Selim, G., & McNamee, D. (1999b). The Risk Management and Internal Auditing Relationship: Developing and Validating a Model. *International Journal of Auditing*, *3*(3), 159–174. https://doi.org/10.1111/1099-1123.00057

Souza, F. S. R. N. de, Braga, M. V. de A., Cunha, A. S. M. da, & Sales, P. D. B. de. (2020). Incorporação de modelos internacionais de gerenciamento de riscos na normativa federal. *Revista de Administração Pública*, *54*(1), 59–78. https://doi.org/10.1590/0034-761220180117

Trapp, A. C. G., & Corrar, L. J. (2005). Avaliação e gerenciamento do risco operacional no Brasil: análise de caso de uma instituição financeira de grande porte. *Revista Contabilidade & Finanças*, *16*, 24–36.

Vanderlei, S. (2022). *O processo de institucionalização da política de gestão de riscos na administração pública federal direta: estudo de caso do Ministério da Justiça e Segurança Pública*. Fundação Getúlio Vargas, Brasília.

Vieira, J. B., & Araújo, A. B. (2020). Risk management in the Brazilian Federal Government: a ministerial analysis. *Revista Do Serviço Público*, *71*, 404–437. https://doi.org/10.21874/rsp.v71ic.4466

Vieira, J. B., & Barreto, R. T. de S. (2019). *Governança, gestão de riscos e integridade*. Brasília: Enap.

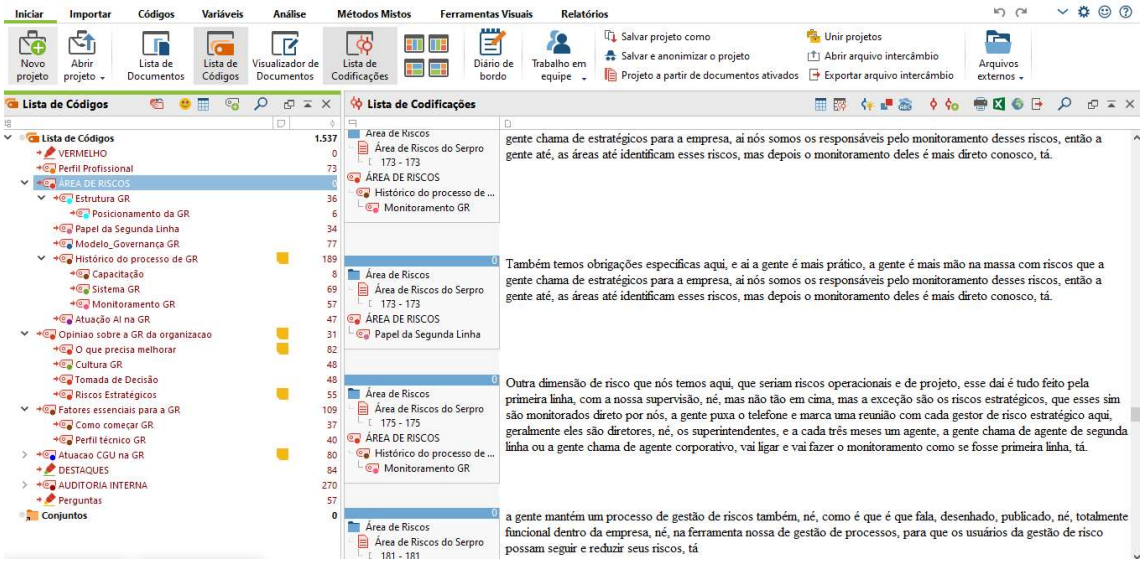
Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, *20*(1), 69–81. https://doi.org/https://doi.org/10.1016/j.mar.2008.10.003

Yin, R. K. (2010). *Estudo de Caso: Planejamento e Métodos* (4th ed.; Bookman, Ed.). Tradução Ana Thorell.

7. ANEXO I

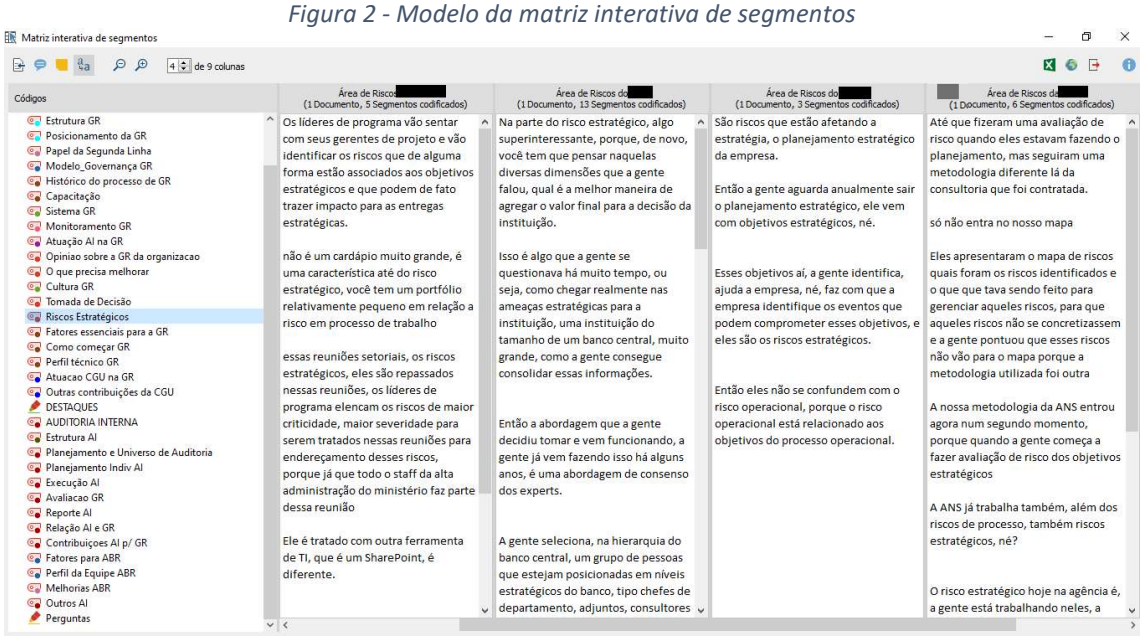
As etapas de codificação no MAXQDA e no Excel das nove entrevistas realizadas no Microsoft Teams, gravadas e, posteriormente, transcritas no software Reshape podem ser evidenciadas nas figuras a seguir.

Figura 1 – Processo de codificação das entrevistas



Fonte: elaboração própria, com apoio do software MaxQDA

Figura 2 - Modelo da matriz interativa de segmentos



Fonte: elaboração própria, com apoio do software MaxQDA

Figura 3 – Refinamento da codificação no Excel

Variáveis	Área de Riscos do	SINTÉSE
	eu falei, até o apetite vai ser dado pela tipologia.	
Relação da GR com a Auditoria Interna / Atuação da AI na GR	Existe a primeira relação que é quando a auditoria trata o processo de gestão de riscos como mais um processo a ser auditado. Mas existe uma outra questão, que é quando eles se utilizam das informações da GR da organização para o planejamento das auditorias baseadas em riscos. Neste caso, ela é usuária do processo de gestão de riscos. E existe o terceiro nível que está começando agora, que é o de reporte, então esse mesmo relatório de relato, além de apresentar para as diretorias trimestralmente apresenta-se também para a auditoria. Nas auditorias, eles são cuidadosos para auditar assuntos que a gente está precisando mesmo se desenvolver. Eles não ficam repetindo a mesma auditoria. "Eles vão vendo a gente e aí eles apontam, olha, sua matriz de calor não está legal". Ou "você precisa diminuir a quantidade de probabilidade de impacto de risco médio". As auditorias de avaliação são úteis porque empurram para frente, através das solicitações de auditoria e das recomendações de auditoria.	1) AI utiliza as informações da GR para o seu planejamento das auditorias 2) Auditam processos que a organização precisa mesmo desenvolver 3) As auditorias de avaliação da GR são úteis porque suas recomendações são sempre melhorias no processo de GR

Fonte: elaboração própria

Figura 4 – Refinamento da codificação no Excel

Tópicos	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	TOTAL
Que fatores são necessários											
Envolver a alta administração	S	S		S		S	S	S	S		7
Envolver as pessoas			S		S						2
Desenvolver a cultura de riscos	S	S	S		S						4
Ter planejamento estratégico				S							1
Ter um sistema de TIC para gestão de risco								S			1
Fazer capacitação contínua do corpo funcional						S					1
Regulamentação do processo de gestão de riscos			S	S		s					3
Definir o apetite a riscos									S		1
Ter as três linhas de defesa atuando		S									1

Fonte: elaboração própria