

Gestão de riscos estratégicos: Uma abordagem adaptativa para ambientes dinâmicos

Tiago Chaves Oliveira¹, Eveline Martins Brito², Olavo Venturin Caldas³ e Bianca Cristina Lessa Enders⁴

Resumo: A gestão de riscos estratégicos é um tema fundamental para a sustentabilidade das organizações, especialmente em contextos marcados por mudanças frequentes e alta complexidade. Este relato apresenta a experiência da Controladoria-Geral da União (CGU) na implementação de uma abordagem adaptativa de gestão de riscos, integrado o modelo de gestão por Objetivos e Resultados Chaves (*Objectives and Key Results* - OKR), adotado para o planejamento institucional. O modelo reconfigurou o papel do risco no processo decisório, tornando-o orientado por valor. Os resultados obtidos mostram maior efetividade e aderência da gestão de riscos à prática institucional. O relato detalha os desafios enfrentados, as soluções adotadas, os impactos alcançados e os desdobramentos futuros esperados.

Palavras-chave: Gestão de riscos; planejamento estratégico; OKR; setor público; governança adaptativa.

1. Auditor Federal de Finanças e Controle, Diretor de Planejamento, Inovação e Sustentabilidade da Controladoria-Geral da União (CGU). Mestre em Governança e Desenvolvimento com especialização em Gestão de Projetos e Bacharel em Ciência da Computação. É certificado em Auditoria Governamental (CGAP do IIA) e em Gerenciamento de Projetos (PMP do PMI). É autor do Guia de Gerenciamento de Portfólios e Projetos do Governo Federal. Condecorado em 2020 pelo Project Management Institute (PMI) como um dos 50 profissionais do mundo da nova geração de talentos em projetos (Future 50). Está à frente do laboratório de inovação da CGU. Foi gestor do time do Robô Alice da CGU, premiado em 3 diferentes premiações nacionais de inovação. Já representou o Brasil em delegações oficiais em discussões ligadas à função de auditoria interna na OCDE e na ONU. Atua nas temáticas de Inovação, Auditoria Interna, Gerenciamento de Projetos e de Riscos como praticante, professor e facilitador.

2. Servidora de carreira da Controladoria-Geral da União e atual Secretária-Executiva da CGU. Ocupou o cargo de Secretária Federal de Controle Interno Adjunta, Ouvidora da Presidência da República, além de cargos na Corregedoria-Geral da União e de gestão. É Engenheira Agrônoma e bacharel em Direito. Tem Pós-Graduação em Legislativo e Políticas Públicas. Ingressou no serviço público em 1994 e, desde 2002, é Auditora Federal de Finanças e Controle. Atua há mais de vinte e cinco anos na área de auditoria, com experiência também em gestão pública, corregedoria e ouvidoria.

3. Doutor em Ciências Contábeis pela Universidade de Brasília/DF (2020). Atuou na CGU/DF (2005/2016) nas áreas de Correição, Prevenção à Corrupção, Transparência e Informações Estratégicas e na CGU/ES em auditoria (2016/2020), exercendo as funções de Coordenador-geral e Chefe de Divisão. Foi Subsecretário de Tecnologia da Informação na Prefeitura Municipal de Vitória/ES (2021/2022). Superintendente da CGU/ES (2023). Diretor de Investigação e Operações na SFC/CGU (2024). E ocupa o cargo de Secretário Executivo Adjunto da Controladoria Geral da União (nov/2024). Atua, ainda, como professor dos cursos de Pós-graduação na Fucape Business School desde 2018.

4. Auditora Federal de Finanças e Controle com uma trajetória sólida e dedicada de mais de 19 anos de experiência no serviço público. Atualmente ocupa o cargo de Diretora de Gestão Corporativa da Secretaria-Executiva da Controladoria-Geral da União (CGU). Tem experiência em compras públicas, inclusive atuou como pregoeira da CGU. Ao longo de sua carreira profissional, se destacou em trabalhos de auditoria que visaram o aperfeiçoamento da gestão, especialmente na temática de logística pública, contribuindo para um serviço público mais eficiente e transparente.

1. INTRODUÇÃO

A gestão de riscos tem se consolidado como um elemento estratégico da governança organizacional, sendo cada vez mais reconhecida como ferramenta essencial para a melhoria da tomada de decisão, alocação eficiente de recursos e priorização de ações no setor público. Essa consolidação reflete um movimento internacional de difusão de modelos estruturados, como o COSO ERM e a ISO 31000, adaptados à realidade brasileira, mas ainda enfrentando desafios específicos de implementação (Souza et al., 2020, Silva et al., 2021).

No contexto da administração pública, a adoção de metodologias estruturadas de gestão de riscos enfrenta entraves significativos, como a rigidez normativa, a rotatividade das lideranças e a necessidade de compatibilizar diretrizes legais com a realidade operacional das organizações públicas. Essas barreiras são agravadas por culturas organizacionais avessas ao risco e por pressões institucionais que priorizam a conformidade em detrimento da inovação e da aprendizagem (Brown & Osborne, 2013).

Além disso, o tema ainda é considerado incipiente na literatura brasileira, com baixa produção científica sistematizada, o que limita o embasamento técnico e a efetividade da aplicação prática no contexto nacional (Oliveira & Abib, 2023, Silva et al., 2021).

A Controladoria-Geral da União (CGU), exemplifica esse contexto, com 2.578 servidores distribuídos em 7 Secretarias, 28 Departamentos e 103 unidades gestoras, incluindo representações regionais nos 26 estados brasileiros, a instituição atua de forma transversal em políticas de integridade pública e privada, educação cidadã, transparência, auditoria, responsabilização, acordos de leniência, ouvidoria e dados abertos (CGU, 2024). A média de idade dos servidores é de 47 anos, sendo 34% mulheres e 66% homens — perfil que impõe desafios adicionais à modernização institucional e à construção de soluções integradas.

Este relato tem como objetivo apresentar a experiência da Controladoria-Geral da União (CGU) na construção e implementação de um modelo adaptativo de gestão de riscos estratégicos, articulado ao sistema de planejamento baseado em *Objectives and Key Results (OKR)*. A proposta visa responder à seguinte questão de pesquisa: como integrar a gestão

de riscos à estratégia institucional de forma ágil, funcional e orientada a valor em ambientes públicos sujeitos a mudanças frequentes?

O contexto institucional da CGU é caracterizado por uma atuação multifacetada, que abrange desde atividades de educação cidadã, promoção da transparência e dados abertos, ouvidoria, até ações voltadas a auditoria interna, investigação e apuração de irregularidades, processos disciplinares e de responsabilização, bem como a celebração de acordos de leniência (CGU, 2024). Essa atuação transversal, combinada à diversidade de áreas técnicas e à recorrente atualização de prioridades estratégicas, revelou os limites dos modelos tradicionais de gestão de riscos, especialmente no que se refere à sua aplicabilidade prática. O desafio enfrentado pela CGU foi o de alinhar a gestão de riscos aos processos decisórios reais da organização, promovendo sua integração ao planejamento estratégico, sem perder de vista a efetividade e a geração de valor público.

Diante desse cenário, este relato está estruturado em cinco seções principais. A primeira apresenta os fundamentos teóricos da gestão de riscos em ambientes complexos, com base nos principais referenciais internacionais. A segunda seção discute abordagens implícitas e adaptativas de gestão de riscos, com base em evidências da literatura recente. Em seguida, a terceira seção detalha a experiência da CGU na implementação de um modelo próprio de gestão de riscos estratégicos, articulado ao planejamento institucional por OKR. A quarta seção trata da consolidação desse modelo no programa CGU+ Gestão, que institucionaliza práticas integradas de planejamento, desempenho, competências e riscos. Por fim, a última seção apresenta as conclusões e lições aprendidas, destacando as contribuições da experiência da CGU para a modernização da gestão pública em contextos dinâmicos.

1.1 Gestão de riscos em ambientes complexos

A gestão de riscos consolidou-se nas últimas décadas como uma disciplina essencial para a boa governança organizacional, sendo aplicada tanto no setor privado quanto no setor público. Os principais referenciais teóricos utilizados pelas organizações incluem a norma ISO 31000:2018 e o modelo COSO ERM (*Enterprise Risk Management*), que oferecem estruturas amplamente reconhecidas para a identificação, análise, avaliação, tratamento e monitora-

mento de riscos (COSO, 2017; ABNT, 2018; Souza et al., 2020; Silva et al., 2021).

A ISO 31000:2018, norma internacional elaborada pela *International Organization for Standardization*, apresenta diretrizes genéricas para o processo de gestão de riscos aplicável a qualquer tipo de organização. Ela propõe uma abordagem sistemática e integrada, que envolve a definição do contexto, identificação dos riscos, análise, avaliação, tratamento, comunicação e monitoramento. Seu foco está na criação e proteção de valor, e destaca a necessidade de considerar os riscos como parte integrante de todos os processos decisórios e de planejamento (ANBT, 2018).

Já o modelo COSO ERM, amplamente adotado por organizações norte-americanas e por setores regulados, estrutura a gestão de riscos como parte do sistema de governança corporativa, integrando riscos à estratégia e ao desempenho. O COSO enfatiza a importância da cultura de riscos, da definição clara de apetite a risco e do alinhamento entre objetivos organizacionais e as respostas aos riscos identificados (COSO, 2017).

Ambos os modelos partem de uma estrutura lógica clássica para o entendimento dos riscos. Essa estrutura é baseada na tríade: evento de risco, causas e consequências. A essa lógica, somam-se os componentes de probabilidade e impacto, que orientam a avaliação da severidade do risco e subsidiam a priorização de respostas. A metodologia também inclui a identificação e a avaliação de controles existentes, cujo objetivo é mitigar os efeitos negativos ou aumentar as oportunidades.

Embora essas abordagens sejam robustas e bem estruturadas, elas pressupõem certo grau de estabilidade organizacional e disponibilidade de tempo para análise, o que pode representar um desafio para organizações que operam em ambientes marcados por alta volatilidade e mudanças frequentes de prioridades. Em tais cenários, o tempo necessário para documentar cada elemento do risco e analisar controles pode comprometer a agilidade na resposta. Os próprios frameworks mencionados ditam que a eficácia da gestão de riscos está diretamente relacionada à sua capacidade de gerar valor e apoiar a tomada de decisões — e não apenas ao cumprimento de uma sequência rígida de etapas técnicas.

Esse tensionamento entre profundidade analítica e agilidade decisória torna-se ainda mais evidente em instituições públicas que lidam com múltiplas demandas, recursos limitados e uma dinâmica política e institucional em constante transformação. Assim, a aplicação estrita dos modelos tradicionais pode se mostrar inadequada para finalidades de governança estratégica em ambientes reais, como o da administração pública federal brasileira. Esse contexto levou a Controladoria-Geral da União (CGU) a repensar suas abordagens de gestão de riscos, buscando maior funcionalidade e integração com os modelos contemporâneos de planejamento estratégico e entrega de valor.

1.2 Gestão de riscos em abordagens implícitas e adaptativas: evidências da literatura

A literatura recente aponta para a emergência de abordagens não tradicionais de gestão de riscos, especialmente em contextos que demandam agilidade, flexibilidade e resposta rápida a mudanças. Essas abordagens dispensam a identificação formal de riscos e controles (eventos, causas, impactos, probabilidades), operando com mecanismos de monitoramento e adaptação contínuos, integrados à rotina de execução (Bugarová & Šimíčková, 2019). A seguir, são apresentados estudos empíricos que abordam esse modelo.

Garcia, et al. (2022) analisaram 23 estudos sobre práticas de risco em métodos ágeis, a publicação demonstra que a maioria das equipes ágeis já realiza gestão de riscos de maneira implícita, por meio das cerimônias do próprio processo. O artigo destaca que as práticas de gestão de risco estão integradas às atividades regulares e muitas vezes são mais ágeis e efetivas do que as metodologias tradicionais.

Coyle e Conboy (2009), demonstram como a gestão de riscos pode ser efetiva mesmo sem práticas formais. Os autores mostram que os riscos são identificados e tratados ao longo das cerimônias ágeis e que, paradoxalmente, a ausência de rigidez aumenta o engajamento e a efetividade do processo. Em vez de registros formais, o processo se apoia em conversas frequentes, adaptação em tempo real e responsabilização compartilhada.

Ribeiro, et al. (2009) apresentam o modelo GARA (Gestão Ágil de Riscos de Ambiente), no qual os riscos são tratados como impedimentos identi-

cados ao longo da execução dos projetos e comunicados informalmente. O processo não utiliza categorização formal, tampouco avaliação de impacto ou probabilidade. A identificação ocorre por meio da interação entre as equipes, e as decisões são tomadas com base em prioridade estratégica. O foco está na coordenação Inter projetos e na comunicação eficaz, com formalização apenas quando necessária.

Apesar das diferenças nos contextos estudados, os estudos compartilham características relevantes:

- Ausência de identificação formal: Nenhum dos modelos exige o preenchimento de registros formais de eventos, causas, controles ou matrizes de risco.
- Integração com a rotina de execução: A gestão de riscos é realizada de forma contínua e está inserida no fluxo normal de trabalho, principalmente por meio de interações frequentes entre os membros da equipe.
- Foco na adaptabilidade: O foco recai sobre a capacidade de resposta rápida a problemas emergentes, em vez da previsibilidade completa dos riscos.
- Formalização mínima: A documentação é usada apenas quando necessária, muitas vezes em níveis mais altos de governança ou em projetos com maior complexidade institucional.
- Risco como parte da performance: Os riscos deixam de ser um artefato técnico isolado e passam a ser elementos integrados à entrega de valor e à governança estratégica.

Esses achados reforçam que, em contextos de alta complexidade e mudança, a eficácia da gestão de riscos pode estar menos na formalização documental e mais na integração entre execução, monitoramento e decisão. A experiência da CGU se insere nesse conjunto de práticas inovadoras, conforme detalhado na seção seguinte.

2. METODOLOGIA E FERRAMENTAS UTILIZADOS

2.1 O Caso da CGU: Inovação na Gestão de Riscos Estratégicos com OKR

A Controladoria-Geral da União (CGU), órgão de controle interno do governo federal brasileiro, exemplifica a necessidade de adaptação da gestão de riscos a contextos organizacionais dinâmicos. Até 2022, a CGU utilizava uma estrutura de plane-

jamento estratégico baseada no Balanced Scorecard (BSC), aliada a um modelo tradicional de gestão de riscos estruturado a partir do mapeamento detalhado dos processos descritos na cadeia de valor institucional.

Embora robusto do ponto de vista metodológico, esse modelo exigia elevado esforço de implementação: longos ciclos de discussão, alto envolvimento de servidores qualificados e projetos que se estendiam por meses. O resultado era um retrato fiel da realidade do processo em um determinado momento, acompanhado por listas de riscos formalmente construídas — mas de difícil monitoramento na prática. Como consequência, o valor percebido pela alta administração era reduzido, uma vez que o modelo não entregava alertas tempestivos que apoiassem a tomada de decisão no cotidiano.

A partir de 2023, a CGU adotou o modelo *Objectives and Key Results (OKR)*, proposto por Doerr (2019), como principal estrutura de planejamento estratégico. Essa mudança, inspirada por práticas de empresas inovadoras como Google e Meta, conferiu maior flexibilidade e capacidade de adaptação ao planejamento institucional.

A adoção do OKR impulsionou uma revisão completa da metodologia de gestão de riscos estratégicos. O modelo tradicional, baseado nos componentes de evento, controle, probabilidade e impacto, mostrou-se inadequado a um ambiente que exige agilidade, coordenação e entrega de valor em ciclos curtos. Em resposta, a CGU estruturou um modelo mais enxuto, ancorado em dados e evidências, centrado na identificação de “pontos de atenção” — situações com potencial de comprometer os objetivos e resultados-chave monitorados nos OKRs e projetos prioritários.

O novo processo sistemático de acompanhamento dos riscos estratégicos na CGU, fortemente estruturado em dados e evidências, envolve a análise mensal dos OKR estratégicos e dos projetos prioritários. Esse monitoramento contínuo permite identificar, de forma sistemática, “pontos de atenção” que possam comprometer o alcance dos objetivos e dos resultados-chave, que são os riscos estratégicos, de fato. Esses pontos são consolidados em relatórios e submetidos mensalmente aos integrantes do Comitê de Governança Interno (CGI), colegiado composto pelos Secretários e pelo Ministro da CGU.

A prática de gestão de riscos é fortalecida pelo acompanhamento diário pelo Ministro e pela Secretaria-Executiva do desempenho dos principais indicadores da Casa, por meio de painéis desenvolvidos especificamente para este fim e que estão disponibilizados em televisores instalados em seus gabinetes. Essa análise já resultou na solução tempestiva de problemas identificados já na sua origem.

Quadrimestralmente, o CGI realiza reuniões para discutir os principais desafios identificados no monitoramento dos OKR institucionais, incluindo os riscos que podem impactar o alcance dos objetivos. Nessas ocasiões, também são definidas as prioridades para o período subsequente. Além disso, a CGU tem investido em soluções tecnológicas, como painéis de Business Intelligence (BI) para a média gestão e uma página institucional na intranet, para disponibilizar informações gerenciais e estratégicas, facilitando o acompanhamento tempestivo do desempenho e a identificação de riscos por todos os servidores.

3. RESULTADOS E IMPACTOS OBTIDOS

3.1. CGU+Gestão: institucionalizando a gestão adaptativa de riscos

A experiência da CGU com a integração dos OKR institucionais e o monitoramento contínuo de pontos de atenção demonstrou que é possível gerir riscos estratégicos de forma eficaz sem recorrer às estruturas clássicas baseadas em eventos, causas, impactos, controles e probabilidades. Essa abordagem mais leve e funcional abriu caminho para uma transformação mais ampla, atualmente em curso, com a implementação do programa CGU+ Gestão, lançado em 2025.

O programa propõe um novo modelo de gestão institucional, integrando de forma estruturada planejamento, desempenho, competências, desenvolvimento de pessoas, estruturas de governança e sistemas de informação. Seu objetivo é superar a fragmentação entre o que é planejado, executado e avaliado, promovendo coerência entre metas, entregas, responsabilidades e processos de aprendizagem organizacional.

No âmbito da gestão de riscos, o CGU+ Gestão institucionaliza uma abordagem adaptativa e orientada a valor. Em vez de partir da identificação formal

de riscos, a estratégia adota como base os compromissos institucionais registrados nos Planos de Entrega (PE) das unidades (Coordenações-Gerais e Controladorias Regionais nos Estados). Esses compromissos refletem tanto as prioridades do Plano Estratégico Institucional e do Plano de Integridade e Combate à Corrupção quanto as atribuições específicas de cada unidade.

O monitoramento do cumprimento desses compromissos permite a identificação contínua de pontos de atenção, que sinalizam riscos à entrega de valor público. Essa identificação ocorre de forma sistêmica e em diferentes níveis da organização, conectando o cotidiano operacional às metas estratégicas. Com isso, os riscos passam a ser tratados como elementos integrantes do desempenho institucional, e não como registros paralelos ao planejamento.

Além disso, o modelo prevê a definição de metas individuais de desempenho para os servidores, permitindo a construção de planos de trabalho anuais, avaliações transparentes e a elaboração de planos de capacitação personalizados com base em lacunas de competências específicas, relacionadas com as metas das unidades. Essas metas são definidas considerando as atribuições da unidade, as características e competências específicas de cada servidor, e nem sempre correspondem diretamente às metas institucionais registradas no nível da unidade. Ainda que existam vínculos conceituais, trata-se de dimensões complementares, e não necessariamente de um desdobramento formal. Essa abordagem possibilita uma gestão orientada por dados e evidências, conectando o desenvolvimento de pessoas às entregas organizacionais.

A integração dos sistemas de gestão no CGU+ Gestão reflete a adoção de uma lógica gerencial moderna, baseado no aprendizado contínuo e na governança por resultados. A gestão de riscos, nesse contexto, é operacionalizada na prática por meio do acompanhamento das metas e compromissos — um exemplo de gestão de riscos implícita, já reconhecida em ambientes ágeis e destacada na literatura especializada como uma alternativa eficaz para contextos dinâmicos e complexos.

Por fim, cabe destacar o papel das quatro áreas estruturantes de gestão e governança da CGU — gestão corporativa, tecnologia da informação, inteligência estratégica e planejamento, inovação e

sustentabilidade — como pilares que viabilizam a efetividade do modelo proposto. Essas áreas, por meio de entregas e iniciativas sob sua responsabilidade, oferecem suporte transversal e coordenado, contribuindo para que os objetivos estratégicos da instituição sejam alcançados com uma visão integrada, sistêmica e aderente aos princípios da gestão de riscos estratégicos.

4. CONSIDERAÇÕES FINAIS E PRINCIPAIS CONTRIBUIÇÕES

A experiência da Controladoria-Geral da União (CGU) demonstra que, em contextos institucionais marcados por dinâmicas complexas e mudanças frequentes, a gestão de riscos estratégicos tende a ser mais efetiva quando orientada por abordagens adaptativas, integradas e focadas em valor. A adoção de um modelo baseado em acompanhamento dos OKR permitiu à CGU integrar a gestão de riscos ao planejamento estratégico de forma mais funcional e aderente à realidade operacional do órgão. Ressalta-se que o modelo não substitui a necessidade de gerir riscos processuais da maneira tradicional.

Ao substituir a ênfase na estrutura clássica — composta por eventos, causas, impactos, controles e probabilidades — por um sistema centrado em compromissos institucionais monitorados continuamente, a organização passou a identificar riscos a partir de evidências concretas de desempenho, com foco em entregas e resultados. Essa abordagem, mais leve e pragmática, demonstrou maior capacidade de gerar valor para a tomada de decisão e apoiar a atuação das lideranças.

A flexibilidade do modelo OKR, combinada com o uso de ferramentas tecnológicas, o engajamento da alta gestão e a institucionalização de práticas gerenciais integradas no programa CGU+ Gestão, consolidou um ciclo de gestão que une planejamento, desempenho, desenvolvimento de pessoas e mitigação de riscos em uma mesma lógica de valor público.

Essa experiência reforça que a eficácia da gestão de riscos não depende apenas do rigor metodológico, mas da sua capacidade de gerar sentido, orientar decisões e apoiar entregas em contextos reais. Em vez de um fim em si mesmo, o risco passa a ser compreendido como um elemento indissociável do desempenho institucional — e, assim, plenamente incorporado à prática de gestão.

REFERÊNCIAS

- ANBT, 2018. *NBR ISO 31000:2018 - Gestão de riscos - Diretrizes*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.
- Buganová, K., & Šimíčková, J. (2019). Risk management in traditional and agile project management. *Transportation Research Procedia*, 40, 986-993.
- Brown, L., & Osborne, S. P. (2013). *Risk and Innovation*. *Public Management Review*, 15(2), 186 -208. doi:10.1080/14719037.2012.707681
- COSO, 2017. *Enterprise Risk Management: Integrating with Strategy and Performance*. s.l., AICPA.
- Coyle, S. & Conboy, K., 2009. *A case study of risk management in agile systems development*. s.l., s.n., pp. 2567-2578.
- Controladoria-Geral da União. (2024). *Relatório de gestão 2024*. Brasília: CGU. Recuperado de <https://www.gov.br/cgu/pt-br/aceso-a-informacao/auditorias/arquivos/2024/RelatorioGestao2024.pdf>. Acesso em: 31 de julho de 2025.
- Doerr, J. (2019). *Avalie O Que Importa*. Rio de Janeiro: Alta Books, 2019.
- Garcia, F., Hauck, J. & Narloch Rizzo Hahn, F., 2022. *Managing Risks in Agile Methods: a Systematic Literature Mapping*. Pittsburgh, USA, s.n.
- Ribeiro, L., Gusmão, C., Feijo, W. & Bezerra, V., 2009. *A case study for the implementation of an agile risk management process in multiple projects environments*. Portland, Oregon USA , s.n., pp. 1396 - 1404.
- Oliveira, V. G. de, & Abib, G. (2023). Risco na administração pública: uma revisão sistemática focada em uma agenda de pesquisas futuras. *Revista de Administração Pública*, 57(6), e2022-0419. <https://doi.org/10.1590/0034-761220220419>
- Silva, D. A. da, Silva, J. A. da, Alves, G. de F., & Santos, C. D. dos. (2021). Gestão de riscos no setor público: revisão bibliométrica e proposta de agenda de pesquisa. *Revista do Serviço Público*, 72(4), 824-854. Recuperado de <https://revista.enap.gov.br/index.php/RSP/article/view/3991>. Acesso em: 31 de julho de 2025.