CONTROLADORIA-GERAL DA UNIÃO
Comissão de Coordenação de Controle Interno (CCCI)

Desenvolvimento e Consolidação da Gestão de Riscos e Controles Internos na Administração Pública Federal

GRUPO DE TRABALHO
PORTARIA CGU Nº 2.999/2024

março • 2025

CONTROLADORIA-GERAL DA UNIÃO

Setor de Autarquias Sul, Quadra 5 - Bloco A
Brasília - DF / CEP: 70297-400
cgu@cgu.gov.br

Obra atualizada até março de 2025

Diagramação: Coordenação-Geral de Planejamento e Inovação (CGPLA/SFC),
sob supervisão da Assessoria de Comunicação Social • Ascom / CGU

Imagem da capa licenciada por Adobe Stock

CONTEÚDO

INTRODUÇÃO

A Instrução Normativa MP/CGU nº 01, de 10 de maio de 2016, e o Decreto 9.203/2017, normativos produzidos no âmbito do Poder Executivo Federal, instituíram a exigência de implementação da gestão de riscos nos órgãos e entidades federais. No entanto, apesar dos normativos datarem de mais de oito anos, o cenário que se apresenta é diverso: instituições públicas que já realizavam o processo de gestão de riscos e continuaram a avançar; outras que iniciaram sua estruturação e seguem avançando; e, por fim, outras que ainda estão buscando desenvolver e implementar a gestão de riscos.

Desde a publicação da IN MP/CGU nº 01/2016, a Secretaria Federal de Controle Interno (SFC), passou a atuar mais fortemente nos órgãos e entidades da Administração Pública Federal, e até de outros níveis e poderes da federação, por meio de capacitações, fomentando a implementação do processo de gestão de riscos. No entanto, apesar da IN ter estabelecido referenciais conceituais para estrutura de gestão de riscos e controles internos, não foram produzidos, no âmbito da Administração Pública Federal, outros instrumentos, tais como guias práticos para auxiliar na implementação da gestão de riscos. Algumas organizações públicas chegaram a desenvolver metodologias mais robustas, incluindo sistemas informatizados, com disseminação para outras organizações, mas o avanço deste processo não foi uniforme.

Considerando a competência da Secretaria Federal de Controle Interno da Controladoria-Geral da União (CGU), disposta no Decreto nº 11.330, de 1º de janeiro de 2023, de atuar como órgão central do Sistema de Gestão de Riscos e Controle Interno do Poder Executivo Federal; considerando que processos de gestão de riscos já eram objeto de avaliação das unidades de auditoria interna governamental (UAIG), pois é o processo que antecede e define a implementação de controles internos; e considerando, ainda, a competência da CGU, de orientar as atividades relativas à gestão dos riscos à integridade, conforme prevê o Decreto nº 11.529, de 16 de maio de 2023; a Comissão de Coordenação de Controle Interno (CCCI) identificou a necessidade de retomar o fomento do processo de gestão de riscos na Administração Pública Federal de forma mais coordenada.

Para isso, instituiu por intermédio da Portaria CGU nº 2.999, de 16 de setembro de 2024, Grupo de Trabalho com a finalidade de "*elaborar projeto para auxiliar o desenvolvimento e consolidação da Gestão de Riscos e Controles Internos na Administração Pública Federal*".

Segundo a portaria, os resultados do Grupo de Trabalho deveriam ser consolidados em relatório a ser apresentado à CCCI, com os seguintes produtos:

I - diagnóstico da implementação da gestão de riscos na administração direta e indireta;

II - identificação de experiências de implementação que possam contribuir com a sistematização;

III - avaliação de instrumentos de implementação (normativos e ferramentas) existentes na Administração Pública Federal;

IV - proposição de instrumentos de implementação da gestão de riscos na Administração Pública Federal; e

V - instituição de rede de parcerias para fortalecimento da pauta de gestão de riscos.

Nesse sentido, apresenta-se o relatório com os resultados do Grupo de Trabalho.

RESULTADOS

Os trabalhos foram desenvolvidos por meio de uma abordagem estruturada e colaborativa, visando garantir a abrangência e a relevância dos resultados. Para tanto, contemplaram-se, em especial, as seguintes etapas no cronograma de trabalho:

QUADRO 1 – CRONOGRAMA DE TRABALHO

ETAPA	PERÍODO
1. Reuniões de alinhamento	16/09 a 16/12/2024
2. Diagnóstico da implementação da gestão de riscos na administração direta e indireta	16/09 a 24/11/2024
3. Reuniões técnicas com órgão e entidades selecionados	11/10 a 22/11/2024
4. Estudo de normativos e instrumentos de implementação	11/10/2024 a 27/01/2025

I. Diagnóstico da implementação da gestão de riscos na administração direta e indireta e identificação de experiências de implementação que possam contribuir com a sistematização (reuniões técnicas)

O objetivo global do diagnóstico foi obter percepções gerais sobre a gestão de riscos no âmbito de grupo de órgãos e entidades selecionados e fornecer subsídios para o desenvolvimento das atividades do Grupo de Trabalho, sem, entretanto, configurar-se como uma avaliação formal.

Destaca-se que a etapa teve os seguintes objetivos específicos relacionados à compreensão da amostra analisada quanto à gestão de riscos:

a) Verificar a existência de Política de Gestão de Riscos nas instituições públicas;

b) Compreender os diferentes tipos de estrutura das unidades responsáveis pela gestão de riscos;

c) Analisar casos em que há acúmulo de competências de gestão de riscos e de gestão de integridade em uma mesma unidade organizacional;

d) Verificar se o órgão ou entidade definiu riscos à integridade como uma tipologia de risco a ser gerenciada; e

e) Verificar se há adoção de procedimento(s) específico(s) para a gestão de riscos à integridade.

Para essa etapa, o GT baseou-se no levantamento de contexto da gestão de riscos realizado pela Secretaria de Integridade Pública (SIP) da CGU sobre o panorama da gestão de riscos à integridade no Poder Executivo Federal, no âmbito do Modelo de Maturidade em Integridade Pública (MMIP).

Foram analisadas as informações endereçadas por 37 organizações públicas, sendo 16 órgãos da administração direta e 21 entidades da administração indireta.

Não obstante o MMIP estar voltado para a gestão de integridade, os levantamentos e análises realizados no âmbito desse modelo auxiliaram no diagnóstico da implementação da gestão de riscos de forma geral, uma vez que gestão de riscos à integridade e gestão de riscos organizacionais, como um todo, estão igualmente sustentados em prevenção, detecção e correção; sendo a integridade um dos princípios fundamentais da governança corporativa. Os resultados detalhados dessas análises constam do Anexo I deste Relatório.

Em complemento ao levantamento produzido a partir do MMIP, foram considerados os resultados identificados no Índice de Governança e Sustentabilidade (iESGo) do Tribunal de Contas da União (TCU). O iESGo é o remodelamento do Índice de Governança e Gestão (IGG), autoavaliação instituída em 2017, por meio do qual o TCU buscou conhecer melhor a situação da governança na administração pública e estimular suas organizações jurisdicionadas a adotarem boas práticas no tema. Por meio do iESGo, além da Governança, as autoavaliações incluem práticas nas demais dimensões incluídas no conceito de ESG (*Enviromental, Social and Governance*). Dentre as dimensões incluídas, está a de Estratégia, que é formada pela agregação dos seguintes indicadores:

a) Gerir riscos (2110);

b) Estabelecer a estratégia (2120);

c) Promover a gestão estratégica (2130);

d) Monitorar os resultados organizacionais (2140); e

e) Monitorar o desempenho das funções de gestão (2150).

O indicador referente à gestão de riscos é medido pelas seguintes questões:

2111: A estrutura da Gestão de Riscos está definida?

2112: As atividades típicas de segunda linha estão estabelecidas?

2113: O processo de GR está implantado?

2114: Os riscos considerados críticos para a organização são geridos?

2115: A organização executa processo de gestão de continuidade do negócio?

A partir da análise conjunta dos resultados do levantamento de informações da SIP/CGU e dos resultados observados no IESGo, foram selecionadas 12 instituições para a realização de reuniões técnicas, com o objetivo de aprofundar a compreensão acerca do funcionamento empírico do processo de gestão de riscos no âmbito da Administração Pública Federal.

Para a seleção das instituições, foram considerados dados indicativos da respectiva atuação na gestão de riscos. Assim, buscou-se contemplar organizações com práticas aparentemente mais consolidadas e organizações com potencial de aprimoramento. Adicionalmente, buscou-se formar um extrato representativo de diferentes setores da administração pública. Para isso, considerou-se, ainda, a busca por organizações representativas dos seguintes setores: Ministérios, Agências Reguladoras, Instituições Federais de Ensino Superior (IFES), Outras Autarquias e Fundações e Empresas Públicas e Sociedades de Economia Mista.

Diante do exposto, vale pontuar que os dados coletados no diagnóstico podem não refletir plenamente a realidade da maioria dos órgãos e entidades do Poder Executivo Federal, uma vez que as organizações foram selecionadas em razão, entre outros fatores, de apresentarem algum grau de implementação da gestão de riscos, ainda que em diferentes níveis. Dessa forma, os dados referentes às organizações não permitem que sejam realizadas inferências estatísticas, mas são importantes ao passo que serviram para obter percepções gerais sobre a temática e indicativos de caminhos a serem trilhados.

Dados os critérios de seleção apresentados, as organizações selecionadas e que receberam reuniões técnicas foram as seguintes:

QUADRO 2 – INSTITUIÇÕES NAS QUAIS FORAM REALIZADAS REUNIÕES TÉCNICAS

GRUPO	NOME	SIGLA
G1 – Ministérios	Ministério dos Transportes	MTR
	Ministério da Saúde	MS
	Ministério do Meio Ambiente e Mudança do Clima	MMA
	Ministério da Justiça e Segurança Pública	MJSP
G2 – Agências	Agência Nacional de Aviação Civil	ANAC
	Agência Nacional de Transportes Terrestres	ANTT
G3 – IFES	Universidade Federal do Ceará	UFC
	Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte	IFRN
G4 - Outras Aut. e Fund.	Departamento Nacional de Obras Contra as Secas	DNOCS
	Departamento Nacional de Infraestrutura de Transportes	DNIT
G5 - Empresas	Serviço Federal de Processamento de Dados	SERPRO
	Empresa Brasileira de Serviços Hospitalares	EBSERH

Destaca-se que o levantamento inicial buscou analisar aspectos de estrutura e conformidade, com base em documentos. Nesse sentido, as reuniões técnicas realizadas nas organizações selecionadas permitiram que os resultados observados fossem confrontados e enriquecidos pelas entrevistas, possibilitando avaliar qualitativamente a atuação das organizações e validar, ou não, os resultados das análises iniciais.

Antes da condução das reuniões técnicas, foi realizado um processo de benchmarking com duas instituições financeiras — Banco Central do Brasil e Banco do Brasil S/A—, entidades com nível de maturidade em gestão de riscos avançado, com o objetivo de compreender de que forma organizações mais estruturadas poderiam subsidiar pontos a serem abordados nas reuniões técnicas com as instituições selecionadas.

Os resultados do diagnóstico e das reuniões com as 12 instituições citadas no Quadro 2 revelaram que os fatores mais relevantes para a implementação de uma gestão de riscos eficaz foram:

- apoio da alta administração;
- existência de estrutura organizacional dedicada, exercendo o papel da segunda linha;
- equipe capacitada em gestão de riscos;
- política de gestão integrada de riscos, reforçando o modelo das três linhas;
- metodologia de gestão de riscos bem definida; e
- disponibilização de ferramentas computacionais para implementação da metodologia, notadamente com capacidade de registro, monitoramento e comunicação dos riscos.

Observou-se ainda a importância do papel da auditoria em avaliar a eficácia e, principalmente, fomentar o processo de gestão de riscos da instituição.

Foi possível identificar que organizações da administração indireta, especialmente as que lidam com riscos financeiros e de tecnologia da informação, estão em estágio mais avançado de maturidade em gestão de riscos. Contribuem para isso exigências normativas mais robustas sobre o tema e processos mais consolidados nas instituições.

Na administração direta, autarquias[1] e fundações, incluindo instituições de ensino, por outro lado, os processos são menos consolidados e ainda enfrentam dificuldades diversas: falta de patrocínio da alta gestão, muitas vezes vinculada às constantes mudanças de gestão; resistência dos gestores (dificuldade de aculturamento); falta de pessoal capacitado (também vinculado à alta rotatividade de pessoal); etc.

O gerenciamento de riscos nessas instituições funciona melhor em "processos de gestão", ou seja, processos transversais, cujo arcabouço normativo é mais robusto, como, por exemplo, os processos de contratações e de gestão de tecnologia da informação, estabelecidos pelo Ministério da Gestão e Inovação (MGI). Esses processos costumam ter objetivos, metas e indicadores bem definidos; instrumentos de monitoramento; responsáveis e partes interessadas bem definidas; etc.

Verificou-se, ainda, avanço na gestão de riscos à integridade. Uma possível causa para esta realidade é a forte atuação da CGU nas orientações sobre tratamento desse tipo de risco, após o advento da Lei Anticorrupção (Lei 12.846, de 1º de agosto de 2013), regulamentada pelo Decreto nº 8.420, de 18 de março de 2015, e da instituição, em 2021, do Sistema de Integridade Pública do Poder Executivo Federal, que foi posteriormente substituído pelo do Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal, com a publicação do Decreto nº 11.529, de 16 de maio de 2023, assim como em virtude da definição de unidades responsáveis pela gestão da integridade, transparência e acesso à informação, sendo as assessorias especiais de controle interno na administração pública direta e unidades formalmente instituídas nos órgãos e entidades da administração indireta.

Outro aspecto identificado foi a semelhança de processos de gestão de riscos em instituições do mesmo grupo: instituições de ensino e agências reguladoras, por exemplo, o que indica que a formação de uma rede, ou a inclusão dessa temática em rede já existente, pode auxiliar no fomento desse processo.

1. O Banco Central do Brasil é uma exceção já que possui uma gestão de riscos madura e em linha com as melhores práticas internacionais

II. Instrumentos de implementação (normativos e ferramentas) da gestão de riscos existentes na Administração Pública Federal

A gestão de riscos na Administração Pública Federal é abordada por um conjunto de normativos/referenciais técnicos que estabelecem conceitos, diretrizes, responsabilidades e procedimentos para melhorar a eficiência da gestão pública. Entre esses normativos, destacam-se:

1. Decreto-Lei nº 200, de 25 de fevereiro de 1967

a) Institui a base estrutural da administração pública federal, dividida em Administração Direta e Indireta, abrangendo órgãos centrais, autarquias, fundações, empresas públicas e sociedades de economia mista; e

b) Destaca a racionalização do trabalho administrativo mediante simplificação de processos e supressão de controles que se evidenciarem como puramente formais ou cujo custo seja evidentemente superior ao risco.

A AGU e o MGI vêm promovendo debates sobre a revisão desse normativo. É um Decreto-Lei anterior à Constituição-Federal, mas que traz questões estruturantes fundamentais da organização da Administração Pública.

2. Decreto nº 3.591, de 6 de setembro de 2000

a) Dispõe sobre o Sistema de Controle Interno do Poder Executivo Federal, estabelecendo suas finalidades, atividades, organização e competências;

b) Embora o Decreto não use explicitamente o termo "gestão de riscos", a previsão de auditorias e avaliações implica a necessidade de identificar e mitigar riscos que possam comprometer a eficiência administrativa e o cumprimento das metas governamentais.

Considerando a instituição do Sistema de Gestão de Riscos e Controles Internos, por meio do Decreto nº 11.330/2023, verifica-se a necessidade de revisão do Decreto nº 3.591/2000.

3. Lei nº 10.180, de 6 de fevereiro de 2001

a) Estabelece a organização de cinco sistemas fundamentais para a gestão pública federal: Sistema de Planejamento e de Orçamento Federal (SPOF); Sistema Federal de Programação Financeira (SFPF); Sistema Federal de Contabilidade (SFC); Sistema de Controle Interno do Poder Executivo Federal (SCI); Sistema de Administração Financeira Federal (SIAFI); e

b) Define as atribuições dos órgãos centrais responsáveis pela supervisão, normatização e coordenação desses sistemas, assegurando a gestão integrada dos recursos públicos e a transparência na administração financeira federal.

Considerando a instituição do Sistema de Gestão de Riscos e Controles Internos, Decreto nº 11.330/2023, verifica-se a necessidade de atualização dessa Lei, para atualização da organização e das competências desse Sistema.

4. Lei nº 12.846, de 1º de agosto de 2013 (Lei Anticorrupção)

a) Disciplina a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública; e

b) Incentiva a adoção de programas de integridade, incluindo mecanismos de gestão de riscos.

5. Instrução Normativa MP/CGU nº 01, de 10 de maio de 2016

a) Estabelece critérios para a implementação de controles internos, gestão de riscos e governança no âmbito da Administração Pública Federal direta, autárquica e fundacional;

b) Prevê a necessidade de identificar, avaliar e mitigar riscos que possam comprometer os objetivos institucionais;

c) Identifica como responsabilidade da alta administração o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão, sem prejuízo das responsabilidades dos gestores dos processos organizacionais e de programas de governos nos seus respectivos âmbitos de atuação;

d) Reforça que a gestão de riscos deve ser integrada ao processo decisório, promovendo uma administração eficiente e transparente;

e) Permite a implantação progressiva de mecanismos de gestão de riscos, de acordo com as características e especificidades de cada órgão ou entidade; e

f) Busca a mitigação de riscos que possam prejudicar a execução de políticas públicas e comprometer a integridade dos recursos públicos.

6. Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais)

a) Estabelece regras de governança corporativa e transparência para empresas estatais; e

b) Determina a necessidade de implementar práticas de gestão de riscos nas atividades das empresas públicas e sociedades de economia mista.

7. Instrução Normativa nº 3, de 09 de junho de 2017

a) Estabelece os princípios, diretrizes e requisitos fundamentais para a prática profissional da auditoria interna governamental no âmbito do Poder Executivo Federal; e

b) Reforça que a estrutura de controles internos dos órgãos e das entidades da Administração Pública Federal deve contemplar três camadas.

- A primeira camada é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos,

contempla os controles primários, que devem ser instituídos e mantidos pelos gestores responsáveis pela implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio.

- A segunda camada é destinada a apoiar o desenvolvimento dos controles internos da gestão e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da primeira. Os Assessores e Assessorias Especiais de Controle Interno (AECI) nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações.
- A terceira linha de defesa é representada pela atividade de auditoria interna governamental. As Unidades de Auditoria Interna Governamental devem apoiar os órgãos e as entidades do Poder Executivo Federal na estruturação e efetivo funcionamento da primeira e da segunda linha de defesa da gestão, por meio da prestação de serviços de consultoria e avaliação dos processos de governança, gerenciamento de riscos e controles internos.

Importante ressaltar que essa Instrução Normativa revogou a Instrução Normativa CGU nº 1, de 6 de abril de 2001, que já trazia diretrizes para a atividade de auditoria interna governamental, com o papel de avaliação de controles internos, definindo o controle interno administrativo como atividades que visam assegurar o atingimento dos objetivos das unidades e entidades da organização. Essa IN já destacava, embora de forma implícita, a importância do processo de gestão de riscos ao estabelecer que quanto maior for o grau de adequação dos controles internos administrativos, menor será a vulnerabilidade dos riscos inerentes à gestão propriamente dita.

8. Decreto nº 9.203, de 22 novembro de 2017 (Política de Governança Pública)

a) Define princípios, diretrizes e práticas para a governança pública.

b) Estabelece que o controle é um dos mecanismos para o exercício da governança pública, que compreende processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos; e

c) Determina a implementação e a manutenção da gestão de riscos e controles como ferramenta para a melhoria da governança pública.

9. Portaria CGU nº 1.089, de 25 de abril de 2018

a) Dispõe sobre a estruturação, execução e monitoramento dos programas de integridade nos órgãos e entidades do Poder Executivo Federal; e

b) Define a gestão de riscos como uma das etapas fundamentais dos programas de integridade.

10. Decreto nº 10.153, de 3 de dezembro de 2019 (Programa Nacional de Prevenção à Corrupção)

a) Institui medidas para prevenir a corrupção no setor público; e

b) Recomenda a adoção de boas práticas de gestão de riscos em processos administrativos.

11. Decreto nº 11.330, de 1º de janeiro de 2023

a) Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Controladoria-Geral da União e remaneja cargos em comissão e funções de confiança; e

b) Estabelece que a CGU é o órgão central do Sistema de Gestão de Riscos e Controles Internos do Poder Executivo Federal.

12. Decreto nº 11.529, de 16 de maio de 2023

a) Institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal (Sitai) e estabelece a Política de Transparência e Acesso à Informação no âmbito federal;

b) Define o programa de integridade como um conjunto de princípios, normas, procedimentos e mecanismos destinados à prevenção, detecção e remediação de práticas de corrupção, fraudes, irregularidades e outros desvios éticos que possam afetar a confiança e a reputação institucional; e

c) Estabelece que as unidades setoriais do Sitai, responsáveis pela gestão da integridade, transparência e acesso à informação, são as assessorias especiais de controle interno na administração pública federal direta, e unidades designadas nas entidades autárquicas e fundacionais.

13. Lei nº 14.600, de 19 de junho de 2023

a) Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, além de alterar alguns normativos. Para a CGU, essa Lei traz a competência de suporte à gestão de riscos (artigo 49, inciso X).

III. Outros normativos que abordam o tema gestão de riscos em processos específicos

14. Decreto nº 9.991, de 28 de agosto de 2019

a) Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da administração pública federal direta, autárquica e fundacional; e

b) Estabelece que as unidades de gestão de pessoas responsáveis pela elaboração, pela imple-

mentação e pelo monitoramento do Plano de Desenvolvimento de Pessoas (PDP) realizarão a gestão de riscos das ações de desenvolvimento prevista.

15. Lei nº 14.129, de 29 de março de 2021

a) Órgãos e as entidades deverão estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e de controle interno com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos da prestação digital de serviços públicos que possam impactar a consecução dos objetivos da organização no cumprimento de sua missão institucional e na proteção dos usuários;

b) Integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

c) Estabelecimento de controles internos proporcionais aos riscos, de modo a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

d) Utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de governança, de gestão de riscos e de controle.

16. Lei nº 14.133, de 1º de abril de 2021

a) A Lei de Licitações e Contratos Administrativos, especificamente o Capítulo III do Título IV dessa Lei, artigos 169 ao 173, dispõe sobre o controle das contratações, estabelecendo que as contratações devem submeter-se a práticas de gestão de riscos e de controle preventivo, inclusive com a adoção do modelo das três linhas

17. Portaria SEGES/ME nº 8.678, de 19 de julho de 2021

a) Dispõe sobre a governança das contratações públicas no âmbito da Administração Pública federal direta, autárquica e fundacional; e

b) estabelece que Caderno de Logística da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia estabelecerá metodologia para a gestão de riscos do metaprocesso de contratação pública.

18. Lei 14.802, de 10 de janeiro de 2024 (PPA 2024-2027)

a) Lei que instituiu o Plano Plurianual da União para o período de 2024 a 2027, indicando os objetivos, metas e indicadores para cada política pública. Ou seja, é a Lei que traz elementos fundamentais para avaliação de riscos, os objetivos.

IV. Referenciais técnicos

19. Avaliação de Políticas Públicas - Guia Prático de Análise *Ex-Ante* (Casa Civil, CGU, Ministério da Fazenda, Ministério do Planejamento, Desenvolvimento e Gestão, 2018)

a) Guia prático que apresenta orientações para avaliação de Políticas Públicas, antes da sua implementação;

b) Apresenta orientações práticas das principais etapas para o desenho, a implementação e a análise de impactos de ações do governo federal, além de trazer informações sobre os principais estágios da construção de políticas; e

c) No que se refere a Gestão de Riscos, o guia traz que, ainda na formulação da política, os responsáveis devem explicitar como seria estruturado o processo de gestão de riscos, cuja finalidade é garantir a existência de mecanismos que permitam a consecução dos resultados almejados.

20. Guia para orientação das atividades das Assessorias Especiais de Controle Interno (CGU, 2023)

a) Orienta as atividades desenvolvidas pelas equipes da Assessoria Especial de Controle Interno (AECI) e apresenta boas práticas desenvolvidas em diferentes ministérios; e

b) Destaca os principais processos de trabalho que fazem parte das atribuições da AECI, entre eles: promoção da gestão de riscos e dos controles internos; auxílio à elaboração da política da gestão de riscos, à definição e à gestão de riscos utilizada, à elaboração e à revisão do Manual de gestão de riscos e controles internos; e avaliação da maturidade em gestão de riscos.

21. Modelo de Maturidade em Integridade Pública (CGU, 2023)

a) O Modelo de Maturidade em Integridade Pública (MMIP), instituído pela CGU, inclui, em seus níveis de maturidade, processos-chave que buscam garantir a existência de critérios mínimos para o estabelecimento das capacidades organizacionais. Nesse contexto, o Modelo conta com macroprocessos-chave relacionados à gestão de riscos, avançando especificamente na gestão de riscos de integridade.

22. Cartilha sobre Gestão de Riscos do Plano de Desenvolvimento de Pessoas – PDP (Ministério da Gestão e Inovação em Serviços Públicos, 2023)

a) Orientações aos órgãos e entidades da Administração Pública Federal sobre como implementar a Gestão de Riscos do Plano de Desenvolvimento de Pessoas.

23. Referenciais Técnicos de Gestão de Riscos (TCU)

a) O Tribunal de Contas da União (TCU) oferece orientações e guias práticos, como o Referencial Básico de Governança e Gestão de Riscos, para orientar órgãos públicos na implementação de práticas de gestão de riscos.

24. Norma ISO 31000 (Aplicação Referenciada)

a) Embora não seja um normativo específico, é amplamente adotada como referência técnica para a gestão de riscos no setor público.

b) Norma da *International Organization for Standardization* que estabelece princípios e orientações genéricas sobre gestão de riscos. A norma traz um *framework* universal para tornar possível o gerenciamento de processos de diversos tipos de riscos de qualquer organização de qualquer segmento independentemente do tamanho e, assim com o COSO ERM, é utilizada de modelo para diversas entidades.

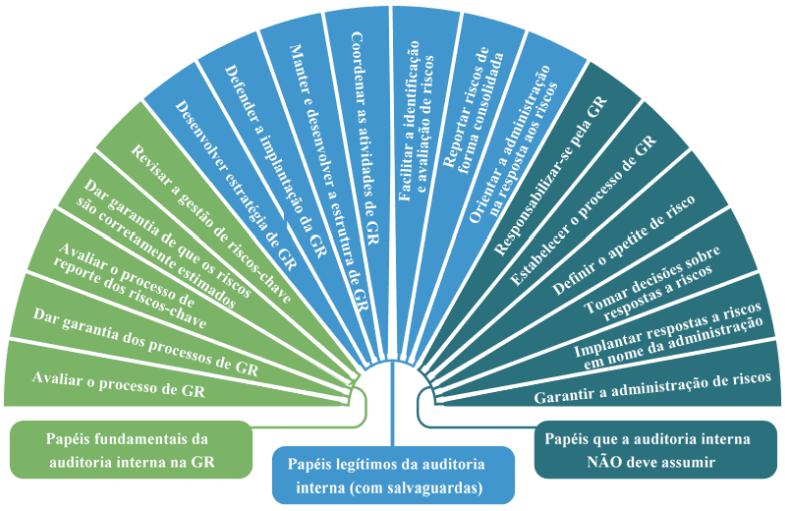
25. COSO ERM

a) Modelo de Gestão de Riscos corporativos, que foi referência para a elaboração de normativos (como a IN 01/2016) e que serve de guia para a instituição do processo em diversas entidades da Administração Pública.

26. Declaração de posicionamento do IIA: O papel da Auditoria interna no gerenciamento de riscos corporativo

a) Documento voltado para a Auditoria Interna, e não ao processo de gerenciamento de riscos em si, mas pode ser observado pelos auditores internos, de forma a garantir a independência e objetividade da auditoria interna e não incorrer em cogestão;

b) Resume papéis que são fundamentais da Auditoria Interna, em relação ao gerenciamento de riscos, papéis legítimos, mas que devem ser realizados com salvaguardas e papéis que a auditoria interna não deve assumir;



c) A atividade de auditoria interna está qualificada para atuar como um defensor e até mesmo como gerente do projeto de gestão de riscos, especialmente nos primeiros estágios de sua implantação. À medida que a maturidade de risco da organização evolua e o gerenciamento de riscos torna-se mais inserido nas operações do negócio, o papel da auditoria interna no gerenciamento de riscos pode ser reduzido.

IV. Ferramentas de apoio à gestão de riscos existentes na Administração Pública Federal

27. ÁGATHA

Sistema de Gestão de Riscos e Integridade, desenvolvido pelo então Ministério do Planejamento, e lançado em 2018. Foi adotado pelo Ministério da Economia, como instrumento oficial para gestão de riscos, em 2020 e seguiu sendo compartilhado com outros órgãos da Administração Pública (inclusive de outras esferas de governo e empresas estatais).

Em 2022 deixou de ser uma solução compartilhável como *software* público. Essa decisão foi tomada na época pelo Ministério da Economia, pela falta de capacidade operacional daquela pasta em oferecer o suporte que era requerido pelos usuários (como apoio para instalação e manutenção da ferramenta). Ainda assim, destaca-se que a ferramenta seguiu sendo disponibilizada aos órgãos interessados, através do encaminhamento do código-fonte pelo MGI, atual gestor do sistema.

Em 2023, após a contratação de empresa (fábrica de software) terceirizada, foram iniciadas melhorias no sistema. A previsão para entrada em produção dessa nova versão é fevereiro de 2025. Dentre as melhorias implementadas, destaca-se a implementação da funcionalidade "multiórgãos", ou seja, poderá vir a ser utilizada por diversos ministérios, sendo hospedado e sustentado pelo MGI. A expectativa do MGI é oferecer o novo Ágatha (multiórgãos) inicialmente aos 13 ministérios atendidos pelo ColaboraGov.

28. AGIR

O sistema AGIR (Aplicativo de Gestão da Integridade e Riscos) é uma solução tecnológica desenvolvida em 2019 pelo Ministério da Justiça e Segurança Pública (MJSP), para apoio ao gerenciamento de riscos. Conforme relatado pelo próprio Ministério, o AGIR é uma ferramenta essencial para a gestão de riscos, fortalecendo a resiliência do Ministério diante de incertezas na execução de políticas, programas e projetos.

O AGIR é baseado em marcos legais como a Instrução Normativa Conjunta CGU/MP nº 1/2016, o Decreto 9.203/2017 e as Portarias nº 76/2021 e 02/2022 do MJSP; além de *frameworks* como o COSO (*Committee of Sponsoring Organizations*) e a norma ISO 31000. Esses instrumentos estabelecem a fundamentação e fornecem estruturas e modelos para a gestão de riscos, garantindo a sua eficácia e eficiência.

O sistema ainda está sendo utilizado pelo MJSP e há tratativas para cessão do código fonte para outro Ministério e para um Estado.

29. e-CGU

Sistema desenvolvido na Secretaria Federal de Controle Interno, em 2019, incialmente de apoio às Auditorias da CGU (e-Aud), posteriormente ampliado para auditorias de outros órgãos. Em 2020, ampliado para apoio às atividades de Gestão Interna da CGU.

O desenho inicial do sistema contava com um módulo capaz de realizar o mapeamento de riscos e operacionalizar a classificação dos riscos. Funcionalidades ainda não finalizadas no sistema.

CONCLUSÃO

A gestão de riscos eficaz deve ter um papel dual na organização: ser capaz de controlar a exposição aos riscos em linha com o apetite e agregar valor ao processo decisório aumentando a probabilidade de atingimento dos objetivos estratégicos.

Verificou-se que as instituições públicas realizam esse processo de avaliação de riscos, mitigando por meio de controles e considerando os riscos na tomada de decisão, porém, muitas delas, o fazem de forma não sistematizada e não integrada, o que dificulta e onera o processo.

Em alguns processos de trabalho transversais, o gerenciamento de risco é mais sistematizado, visto que são conformizadas por outros órgãos de Centro de Governo. Nos exemplos citados neste Relatório, o MGI é protagonista na normatização, induzindo diretrizes sobre o tema, apresentando os principais riscos e sugerindo controles, como, por exemplo, a Lei 14.133/2021, que dispõe sobre licitações e contratos, a Portaria SEGES/MGI nº 7.383/2023, que dispõe sobre transferências de recursos da União, normativos sobre o Sistema de Pessoal Civil da Administração Federal (SIPEC) e sobre o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

Já em relação a processos finalísticos, verificou-se que a gestão de riscos enfrenta dificuldades, principalmente em:

- formalização de área específica para coordenação do processo de gestão de riscos, exercendo o papel da segunda linha;
- recrutamento de equipe capacitada;
- estabelecimento de política de gestão integrada de riscos;
- estabelecimento de metodologias capazes de implementar suas políticas;
- declaração de apetite por riscos;
- apoio da alta administração; e
- disponibilização de ferramentas computacionais para implementação da metodologia, notadamente com capacidade de registro, monitoramento e comunicação dos riscos.

Sobre o arcabouço normativo, verificou-se que há disposições atribuindo aos gestores a responsabilidade pelos processos de gerenciamento de riscos e de controles internos. Também há normativos atribuindo à auditoria interna a avaliação desses processos, além da possibilidade de a auditoria interna assumir o papel de fomento à gestão de riscos, especialmente nos primeiros estágios de sua implantação. Por outro lado, observou-se a necessidade de intensificar as capacitações e avaliações sobre o tema de forma contribuir para a sistematização e aculturamento desse processo.

Ademais, com a instituição do Sistema de Gestão de Riscos e Controles Internos, torna-se necessária a revisão dos atos normativos que tratam do até então Sistema de Controle Interno, em especial a Lei 10.180/2001 e o Decreto 3.591/2000, bem como outros normativos correlatos.

Com relação à gestão de riscos à integridade, verificou-se a relevância da atuação da CGU, por meio da Secretaria de Integridade Pública no fomento à política de integridade, com definição normativa de estrutura e disseminação de práticas, induzindo o processo de forma objetiva. Foi possível observar que há práticas que podem ser adotadas como referência para os encaminhamentos resultantes deste Grupo de Trabalho. Por exemplo, foi verificada importante interação entre áreas responsáveis pela gestão de riscos e pela gestão de integridade, o que tem impulsionado a gestão de riscos à integridade, fortalecendo a gestão de riscos, como um todo, da organização. Tal observação parece derivar da existência de disposições claras sobre o papel das unidades setoriais de integridade por parte da CGU enquanto Órgão Central do Sitai.

Da mesma forma, observou-se que a disposição da CGU em orientar a gestão de riscos à integridade ao longo dos últimos anos foi exitosa na garantia da incorporação dessa tipologia de risco a ser gerenciada nas organizações. Tal ação, indica a capacidade e alcance de resultados quando há orientações claras por parte do Órgão Central. Há que se destacar, por outro lado, que existem divergências entre as metodologias abrangentes de gestão de riscos nas organizações e as metodologias e práticas adotadas para gerenciar riscos à integridade. A harmonização dessas metodologias tende a trazer benefícios para gestão de riscos da instituição, em termos de maior eficiência na coleta, monitoramento, agregação e comunicação da informação de riscos. Assim, é necessário atuar de forma coordenada no âmbito da CGU para que os temas tenham maior interação e integração.

Para fazer frente ao exposto, mostra-se relevante que a CGU coordene ações entre a Secretaria de Integridade Pública e a Secretaria Federal de Controle Interno para a promoção de ações voltadas à integração de suas orientações enquanto órgãos centrais dos respectivos sistemas de integridade e de gestão de riscos e controles internos.

Nas reuniões técnicas realizadas, verificou-se, ainda, a demanda que algumas instituições têm por instrumentalização do processo, de forma mais prática, com a necessidade de orientações mais diretas no sentido de estruturação e até mesmo sistemas de informação. Tal verificação é consistente com as observações relatadas nas considerações do levantamento realizado, na medida em que indicam a necessidade de aprimoramento da atuação do Órgão Central nos temas relacionados à gestão de riscos.

Considerando, então, o atual cenário de estruturação da Administração Pública Federal, o levantamento de contexto da gestão de riscos elaborado no âmbito deste trabalho identificou que há oportunidades de melhoria no processo de Gestão de Riscos dos órgãos e entidades da Administração Pública Federal. Foi possível observar que o fortalecimento do tema é capaz de melhorar os resultados verificados nas organizações, por exemplo, nos indicadores, índices e modelos de maturidade adotados como referência no setor público. Nesse sentido, o Grupo de Trabalho verificou que ainda há necessidade de fomentar a elaboração de Políticas de Gestão de riscos mais efetivas, de tal modo que as organizações tenham diretrizes e responsabilidades claras para seus processos de gestão de riscos.

Diante da competência da CGU como órgão central do Sistema de Gestão de Riscos e Controles Internos da Administração pública Federal, propõe-se:

a) revisão da Lei 10.180/2001 e do Decreto 3.591/2000, e demais normativos que tratem do Sistema de Controle Interno, para conformação com o Sistema de Gestão de Riscos e Controles Internos;

b) revisão da IN 01 MP/CGU nº 01/2016 e avaliação de normativos correlatos para conformação com o Sistema de Gestão de Riscos e Controles Internos;

c) definição de metodologia mínima de gestão de riscos, para utilização por entidades que ainda não conseguiram desenvolver ou avançar nas suas próprias metodologias – Resguardadas as salvaguardas na atuação no processo de gerenciamento de riscos;

d) avaliar a possibilidade de disponibilização de sistema de apoio ao processo de gestão de riscos e controles internos, para utilização, não obrigatória, pelas entidades interessadas;

e) estabelecimento de modelo de maturidade do processo de gestão de riscos, com processos chaves para que as entidades possam seguir avançando no seu processo;

f) orientação quanto ao papel das Auditorias internas e das Assessorias Especiais de Controle Interno no processo de gestão de riscos, especialmente nas instituições em que não há institucionalização da gestão de riscos por meio de uma unidade específica;

g) disponibilização de capacitações e avaliações sobre o tema de forma contribuir para a sistematização e aculturamento do processo de gestão de riscos; e

h) identificação de grupos de instituições com processos semelhantes (por exemplo, IFES), para promoção de redes fomentadoras, ou identificação de redes já existentes para incentivo à inclusão dessa pauta.

Considerando ainda as discussões em andamento para a revisão do Decreto-Lei nº 200/67, entende-se salutar que a CGU participe desses debates, para conformação com o Sistema de Gestão de Riscos e Controles Internos. Será necessário ainda avaliar os normativos relacionados, a fim de analisar os impactos e as alterações decorrentes da instituição desse Sistema e das alterações no Decreto-Lei 200.

Com relação ao item "f" das proposições supra, este GT propõe deliberação que reforça o papel das Auditorias Internas e das Assessorias Especiais de Controle Interno no fomento do processo de gestão de riscos, conforme Anexo II.

gov.br Documento assinado digitalmente
SERGIO FILGUEIRAS DE PAULA
Data: 26/03/2025 14:46:42-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
MARCELA JACOMINY DE AMORIM MENDES
Data: 26/03/2025 14:53:38-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
ANDRE SPENCER DE SOUZA HOLANDA
Data: 26/03/2025 15:16:54-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
JOSE LUIZ BARROS FERNANDES
Data: 26/03/2025 16:32:28-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
PATRICIA ALVARES DE AZEVEDO OLIVEIRA
Data: 26/03/2025 17:06:39-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
PAULO MARCELO SANTANA BARBOSA
Data: 26/03/2025 17:16:26-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
JANAINA LUCAS RIBEIRO
Data: 26/03/2025 17:35:12-0300
Verifique em https://validar.iti.gov.br

ANEXO I • Considerações do diagnóstico quanto à gestão de riscos à integridade

Os dados coletados na etapa de diagnóstico apresentaram um conjunto de observações acerca do processo de gestão de riscos à integridade na Administração Pública Federal. Como destacado anteriormente, em que pese o levantamento não tenha sido realizado em amostra estatística e, portanto, não seja possível extrapolar suas conclusões para o universo de organizações do setor público, é possível observar pontos relevantes para o atendimento dos objetivos deste trabalho. Nesse sentido, apresentamos abaixo os temas de maior destaque, divididos em cinco tópicos:

I. Existência de Política de Gestão de Riscos

A existência de uma Política de Gestão de Riscos não é condição necessária e suficiente para a gestão de riscos à integridade, mas facilita, consideravelmente, o trabalho da Unidade Setorial de Integridade (USI) com essa finalidade, uma vez que esta pode utilizar processos e procedimentos já estabelecidos no âmbito da gestão de riscos aplicável a toda a organização para, por corolário, promover a gestão de riscos à integridade. Nesta perspectiva, o Modelo de Maturidade em Integridade Pública (MMIP), considera a gestão de riscos entre seus macroprocessos-chave e estabelece diferentes níveis de maturidade, conforme estruturação e funcionamento do processo na organização. O Nível-2 Padronizado, por exemplo, inclui aspectos relacionados à estruturação da gestão de riscos presentes na organização, requisitos básicos, porém essenciais, na medida em que contribuem para o estabelecimento e desenvolvimento da gestão de riscos à integridade no âmbito do órgão ou entidade.

Nas 37 organizações que tiveram informações e documentos analisados no âmbito do diagnóstico, foi observado que 97,30% (36) possuem Política de Gestão de Riscos. Em uma organização não foi possível verificar as informações relacionadas a existência do artefato. O dado reflete o cumprimento de obrigação legal imposta pela Instrução Normativa Conjunta nº 01, de 10 de maio de 2016, dado que a norma exige que as organizações do Poder Executivo Federal instituam suas respectivas Políticas de Gestão de Riscos.

Há que se destacar, contudo, que essa situação não se reflete de forma uniforme em todo o Poder Executivo Federal. Isso porque, de acordo com os dados do iESGo, das 291 organizações públicas do Poder Executivo Federal abarcadas pelo índice, 25% responderam ao questionário informando não possuir uma Política de Gestão de Riscos. É possível notar ainda que o resultado do indicador "Gerir riscos (2110)" e a média do iESGo demonstram que há diferença significativa de performance entre as organizações que possuem a Política e as que não a possuem, o que dá indícios da importância do instrumento, conforme quadro abaixo:

	25% QUE **NÃO** POSSUEM POLÍTICA DE GESTÃO DE RISCOS	75% QUE POSSUEM POLÍTICA DE GESTÃO DE RISCOS	TODAS AS ORGANIZAÇÕES (Σ)
Média no Indicador Gestão de Riscos do iESGo (2110)	11,32%	63,04%	49,89%
Média Geral do Índice iESGo	31,91%	61,36%	53,87%

A constatação de que ainda há inadequações em 25% das organizações, mesmo após oito anos de vigência da norma que exige a instituição da respectiva Política de Gestão de Riscos, sublinha a necessidade de ações contínuas para fortalecer a cultura de gestão de riscos, inclusive riscos à integridade, considerando que a primeira fortalece a segunda e que ambas têm por objetivo contribuir para o impulsionamento das entregas públicas. Assim, é necessário que a estratégia a ser construída em razão do presente trabalho leve em consideração a necessidade de fomentar o cumprimento da exigência por parte dos órgãos e entidades que não adotaram medidas de institucionalização de suas Políticas de Gestão de Riscos até o momento.

II. Tipos de estrutura da unidade responsável pela gestão de riscos

Outro ponto analisado diz respeito ao tipo de estrutura responsável pela gestão de riscos na organização. Ou seja, neste tópico buscou-se compreender de que forma a organização funcional da estrutura influencia a os resultados da gestão de riscos. Para tanto, o trabalho verificou que as 37 organizações podem ser agrupadas da seguinte forma:

i. **unidade operacional**, correspondendo a 89,19% (33) do total. Foram classificadas nesse grupo as organizações que indicaram, na autoavaliação do MMIP, unidade da estrutura organizacional, como secretaria, superintendência, diretoria, gerência, coordenação ou AECI, como responsável pela gestão de riscos. Além disso, também foram incluídas nesse grupo as organizações que indicaram comissões ou comitês como responsáveis, mas cujos documentos analisados evidenciaram a existência de uma unidade específica encarregada da operacionalização e implementação do processo de gestão de riscos. No caso das empresas estatais, essas informações foram obtidas em documentos como Políticas de Gestão de Riscos ou Regimentos Internos, uma vez que estas não estão incluídas no escopo da autoavaliação do MMIP.

ii. **comissão, comitê ou núcleo**, correspondendo a 10,81% (4) do total. Neste grupo, foram classificadas as organizações que indicaram comissões, comitês ou núcleos como responsáveis pela gestão de riscos, mas não apresentaram, nos documentos analisados, evidências de uma unidade específica encarregada da implementação do processo. Ou seja, o grupo é composto por organizações em que a gestão de riscos é responsabilidade de uma estrutura de governança em lugar de uma estrutura organizacional.

Com base nessa categorização, buscou-se verificar possíveis relações entre o tipo de estrutura responsável pela gestão de riscos, o desempenho geral da organização no âmbito do iESGo e o desempenho no indicador de Gestão de Riscos (2110):

INDICADOR	UNIDADE OPERACIONAL	COMITÊ/ COMISSÃO/ NÚCLEO
Média no Indicador Gestão de Riscos do iESGo (2110)	64,98%	40,16%
Média Geral do Índice iESGo	65,07%	54,87%

Os dados indicam que a alocação da responsabilidade sobre a gestão de riscos em uma unidade responsável dentro da estrutura organizacional, mesmo que esta também realize outras atividades como controle interno, governança ou planejamento estratégico, está associada a um desempenho

superior nos indicadores do iESGo, tanto no índice de gestão de riscos (coluna 2110 do questionário) quanto no índice geral.

As entrevistas realizadas confirmaram essa percepção, com algumas organizações destacando que quando a responsabilidade pela gestão de riscos é atribuída a comitê ou comissão, sem o suporte de uma unidade específica para coordenar e operacionalizar o processo, os resultados tendem a ser inferiores.

Essa constatação sugere que a institucionalização da gestão de riscos por meio de uma unidade específica na estrutura organizacional não apenas favorece a implementação do processo, como também contribui para melhores resultados. Consequentemente, essa estruturação cria um ambiente propício para a gestão da integridade, pois permite o aproveitamento de processos e metodologias já estabelecidas para a identificação e o tratamento de riscos à integridade, fortalecendo a integração e articulação entre a área responsável pela gestão de riscos e a Unidade Setorial de Integridade. Nesse sentido, a existência de estruturas de governança pode contribuir com a gestão de riscos à integridade, mas os resultados do presente trabalho demonstram que, na amostra analisada, é desejável que o tema seja responsabilidade de uma estrutura organizacional, a qual pode se valer de uma estrutura de governança para maximizar seus resultados.

III. Acúmulo de competências de gestão de riscos e de gestão de integridade

Com relação ao acúmulo de competências de gestão de riscos e de gestão de integridade em uma mesma unidade, o diagnóstico realizado na amostra de 37 organizações revelou que, em 54,05% (20) delas, há acúmulo das atribuições e ambas as funções são desempenhadas pela mesma unidade – considerada unidade em nível de Coordenação-Geral ou inferior. Em 45,95% (17), essas atividades são realizadas por unidades distintas.

Além disso, ao analisar a posição da unidade no organograma em um nível de agregação maior (considerado o nível de diretoria ou superior), observou-se que em 62,16% (23) das organizações a unidade responsável pela gestão de riscos e a unidade responsável pela integridade estão inseridas na mesma estrutura organizacional. Ou seja, a gestão de riscos e a gestão de integridade estão alocadas sob uma mesma estrutura, como uma diretoria ou secretaria. Em contrapartida, 37,84% (14) das organizações essas responsabilidades estão separadas em unidades organizacionais distintas.

Embora essas responsabilidades estejam alocadas em estruturas separadas em 37,84% (14) das organizações, o levantamento no âmbito das 37 instituições também revelou que 100% delas têm a unidade responsável pela gestão de integridade como referência para a gestão de riscos à integridade. Logo, os dados demonstram que, mesmo quando há estruturas hierárquicas apartadas, a gestão de riscos e a gestão de integridade atuam de forma colaborativa em todos os 37 órgãos ou entidades analisados, seja por atuarem na mesma estrutura, seja porque a organização envolveu a USI como referência para a gestão de riscos à integridade. Essa constatação foi corroborada pelas reuniões técnicas, nas quais os órgãos e entidades denotaram o papel proativo da unidade responsável pela gestão de integridade, tanto no fornecimento de conhecimento especializado e apoio à unidade de gestão de riscos, quanto na identificação direta dos riscos à integridade.

Convém frisar que responsabilidade de coordenar a gestão de riscos à integridade é uma competência específica da USI prevista no Decreto nº 11.529, de 16 de maio de 2023. Assim, percebe-se que a definição de papéis de forma clara e direcionada facilita a atuação e a colaboração entre as áreas, proporcionando avanços e ganhos para ambas as atividades.

Cabe destacar ainda que, a partir das reuniões técnicas realizadas, foi observado que algumas entidades tiveram a implementação da gestão de riscos à integridade como ponto de partida para a implementação da gestão de riscos organizacionais. Tal observação demonstra a interrelação entre a gestão de riscos à integridade e a gestão de riscos organizacionais, bem como indica um caminho possível para o fomento do tema nas organizações da Administração Pública Federal.

Assim, considerando que, em 54,05% das organizações, as atividades de gestão de riscos e gestão de integridade são desempenhadas pela mesma unidade operacional, e que, em 62,16% das organizações, essas funções estão alocadas sob uma mesma estrutura hierárquica (em nível de diretoria ou secretaria), além do fato de que, quando as funções estão em estruturas segregadas, as organizações envolvem a USI como referência para a gestão de riscos à integridade, observa-se uma clara tendência de integração e colaboração entre as funções de gestão de riscos e de gestão de integridade. Essa atuação conjunta não apenas fortalece ambas as áreas, como também promove sinergias que contribuem para uma governança mais eficiente e para a construção de uma cultura organizacional orientada ao gerenciamento de riscos e à gestão de integridade. Tal abordagem integrada tende a potencializar os resultados, tanto no âmbito do cumprimento de objetivos estratégicos quanto na mitigação de riscos que possam comprometer a confiança e a credibilidade institucional.

IV. Definição de riscos à integridade como uma tipologia de risco a ser gerenciada

Em que pese o tema de gestão de riscos existir de forma mais estruturada desde 1992, com a publicação do COSO I, a gestão de riscos à integridade é um tema relativamente recente. Como mencionado anteriormente, a Instrução Normativa Conjunta MP/CGU nº 01/2016, por sua vez, estabeleceu o arcabouço para o tema na Administração Pública Federal, apresentando entre suas disposições um conjunto mínimo de tipologias de risco, mas sem considerar os riscos à integridade. Somente a partir de 2017, através do Decreto nº 9.203, de 22 de novembro 2017, houve, pela primeira vez na Administração Pública Federal, a previsão normativa específica sobre a realização da gestão de riscos à integridade. Nesse contexto, faz-se necessário compreender o cenário atual de como os órgãos e entidades estão abordando esse tema em suas Políticas e Metodologias de Gestão de Riscos e em seus Planos de Integridade, em específico se gerenciam os riscos à integridade.

No âmbito do diagnóstico realizado, das 37 organizações, em 97,30% (36) os riscos à integridade estão previstos em seus normativos ou documento orientadores. Em contrapartida, em apenas 2,70% (1) das organizações, essa categoria não foi identificada nas suas políticas ou metodologias.

Esse cenário evidencia um significativo progresso na incorporação dos riscos à integridade nas práticas de gestão de riscos no âmbito do Poder Executivo Federal, com a maioria das organizações estudadas (97,30%) incluindo-os entre os tipos de riscos a serem geridos. Essa evolução, em grande parte, pode ser atribuída a um conjunto de normativos que impulsionaram o tema. Iniciando com a influência positiva do Decreto nº 9.203/2017 e posteriormente da Portaria nº 1.089/2018, que determinou o levantamento e tratamento dos riscos à integridade nos Planos de Integridade dos órgãos e entidades e a constituição de unidades de gestão de integridade. O processo ganhou ainda mais força com a criação do Sistema de Integridade do Poder Executivo Federal (SIPEF) pelo Decreto nº 10.756/2021, que estabeleceu as unidades setoriais de integridade e atribuiu a elas a coordenação da gestão de riscos à integridade. Essa responsabilidade foi mantida pelo Decreto nº 11.529/2023, que revogou o anterior, consolidando o papel da USI nesse processo.

Percebe-se, diante do progresso observado na incorporação dos riscos à integridade nas práticas

de gestão de riscos das organizações analisadas, que a estratégia adotada pela CGU como Órgão Central do SITAI foi exitosa na garantia da incorporação dos riscos à integridade como tipologia de risco a ser gerenciada nas organizações, em que pese não constasse do rol indicado pelo art. 18 da Instrução Normativa Conjunta MP/CGU nº 01/2016. Assim, é possível considerar a estratégia adotada como referência para o fortalecimento da gestão de riscos nas organizações da Administração Pública Federal. Assim, o sistema de gestão de riscos pode se espelhar nesse percurso, adotando estratégias semelhantes de normatização, fortalecimento institucional e coordenação centralizada, de forma a ampliar a abrangência e a efetividade de sua implementação.

V. Adoção de procedimento(s) específico(s) para a gestão de riscos à integridade

Conforme observado no item I, referente à existência de Política de Gestão de Riscos, o diagnóstico revelou que 97,30% (36) das organizações possuem uma Política de Gestão de Riscos formalmente estabelecida. Contudo, esse avanço não se reflete na implementação efetiva do processo de gestão de riscos, que se manifesta pela aplicação de uma metodologia adequada. Não obstante a Instrução Normativa nº 1, de 10 de maio de 2016, determinar que as Políticas de Gestão de Riscos dos órgãos e entidades contemplem diretrizes sobre a utilização de metodologias e ferramentas, a análise da existência ou não de metodologias de gestão de riscos, dentro do universo do diagnóstico, demonstrou que 81,08% (30) das organizações dispõem de tais metodologias, enquanto 18,92% (7) ainda não as desenvolveram.

Ao expandir essa análise para o âmbito do Poder Executivo Federal, com base nos dados de 291 organizações que responderam ao iESGo, referente à pergunta 2112 D – "as atividades da segunda linha incluem o fornecimento de metodologias, ferramentas e orientações em geral para que os gestores da primeira linha identifiquem e avaliem os riscos?", observa-se que 41,23% (120) das organizações não oferecem metodologia, ferramentas e orientações necessárias para a identificação e avaliação de riscos. Esse resultado indica uma lacuna na implementação efetiva do processo de gestão de riscos, o que pode ser considerado um elemento de atenção para as futuras ações da CGU, enquanto Órgão Central, a serem desenvolvidas a partir dos trabalhos deste Grupo de Trabalho.

Ademais, em que pese a metodologia de gestão de riscos da organização devesse, por definição, orientar a identificação e avaliação de riscos das organizações, é possível constatar que há utilização de diferentes instrumentos para gerenciar determinadas tipologias de riscos, como acontece com os riscos à integridade. Essa realidade é observada, inclusive, nas organizações que contam com metodologia de gestão de riscos institucionalizada. Nesse contexto, em relação às metodologias utilizadas, o diagnóstico das 37 organizações apontou que 40,54% (15) conduzem a gestão de riscos à integridade com metodologia própria, utilizando instrumentos como questionários, oficinas e entrevistas. Em 45,95% (17) das organizações, adota-se uma única metodologia da gestão de riscos, que abrange todas as tipologias. Por fim, em 13,51% (5) não foi possível identificar a metodologia utilizada.

Destaca-se, ainda, que a adoção, por um órgão ou entidade, de uma mesma metodologia utilizada na gestão de riscos para tratar tanto os riscos à integridade quanto as demais tipologias de risco sinaliza uma maior maturidade e integração do processo de gestão de riscos da organização. Essa integração é importante, dado que os riscos à integridade são transversais e permeiam diversos processos da organização, devendo, portanto, serem gerenciados no âmbito do macroprocesso de gestão de riscos do órgão ou entidade.

O resultado positivo dessa integração é reforçado ao se comparar o desempenho no iESGo das 17 organizações que utilizam metodologia única de gestão de riscos com as 15 organizações que utilizam metodologia específica para os riscos à integridade:

INDICADOR	METODOLOGIA ÚNICA DE GESTÃO DE RISCOS (17)	METODOLOGIA ESPECÍFICA PARA A INTEGRIDADE (15)
Média no Indicador Gestão de Riscos do iESGo (2110)	73,77%	54,80%
Média Geral iESGo	74,32%	55,68%

Os dados apontam, portanto, que a adoção de uma metodologia de gestão de riscos abrangente, que inclua a tipologia de riscos à integridade ou esteja integrada à gestão desses riscos, está associada a um desempenho significativamente superior no iESGo. Esse resultado reforça as vantagens de se alinhar e integrar metodologias, dada a capacidade de se promover uma visão holística e transversal dos riscos, uma abordagem mais estruturada e consistente, e evitar a duplicação de esforços, resultando em uma gestão mais efetiva.

Cabe destacar ainda informações acerca das características das metodologias de gestão de riscos especificamente elaboradas para abordar riscos à integridade, ou seja, aquelas adotadas quando a organização não se vale da metodologia de gestão de riscos que abranja todas as tipologias de riscos. Entre as organizações analisadas na amostra, destaca-se a aplicação de formulários ou questionários e a realização de oficinas como os procedimentos mais utilizados para a implementação da gestão de riscos à integridade. Essas iniciativas são importantes na medida em que tratam de instrumentos válidos para identificar e priorizar ações no Plano de Integridade, mas não constituem, por si só, um processo maduro de gestão de riscos à integridade.

Nesse contexto, ressalta-se que, embora as ações previstas no Plano de Integridade possam ser fundamentadas em riscos, é importante não confundir o Plano de Integridade com a gestão de riscos à integridade. A atenção a esse ponto se justifica pelo fato de que, durante a análise dos documentos no âmbito do diagnóstico, foi observado que os órgãos e entidades frequentemente utilizam as metodologias mencionadas, entre outras, não apenas como instrumentos para orientar as ações do Plano de Integridade, mas também como ferramentas para identificar e gerenciar riscos à integridade.

Embora essa abordagem inicial seja válida para impulsionar o processo, a gestão de riscos à integridade, quando integrada ao macroprocesso de gestão de riscos da organização, pode gerar resultados mais eficazes e robustos. Desse modo, o Plano de Integridade deve organizar as ações e medidas de integridade a serem adotadas em determinado período, mas nada impede que ele também possa incluir ações já previstas no Plano de Gestão de Riscos, considerando que ambos os processos (os de riscos e os de integridade) têm como objetivo a mitigação de riscos que possam impactar a integridade organizacional.

Por fim, dada a relevância da atuação conjunta, especialmente pela complementariedade das atividades desenvolvidas e pelos resultados positivos advindos da integração de ambas as unidades, a CGU enquanto Órgão Central do Sitai e do sistema de gestão de riscos pode se valer de uma atuação coordenada para a emissão de orientações capazes de impulsionar o assunto na Administração Pública Federal.

ANEXO II • Proposta de Deliberação CCCI

O MINISTRO DE ESTADO DA CONTROLADORIA-GERAL DA UNIÃO, no uso da atribuição que lhe confere o art. 9º, inciso I, do Decreto nº 3.591, de 6 de setembro de 2000, e considerando o disposto nos artigos 19 e 20 do Regimento Interno da Comissão de Coordenação de Controle Interno - CCCI, aprovado pela Portaria nº 1.028, de 22 de abril de 2015, resolve:

Art. 1º Publicar a Deliberação nº 02/2025, da Comissão de Coordenação de Controle Interno - CCCI, aprovada em sessão realizada em XX de XXXX de 2025, na forma do Anexo Único desta Portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

VINÍCIUS MARQUES DE CARVALHO

ANEXO ÚNICO

Deliberação CCCI nº XX/2025: Responsabilidades do Órgão Central do Sistema de Gestão de Riscos e Controles Internos, das UAIG e das AECI no processo de Gestão de Riscos e Controles Internos

A Comissão de Coordenação de Controle Interno, no uso das competências conferidas pelo art. 23 da Lei nº 10.180, de 6 de fevereiro de 2001, e pelo art. 3º do Regimento Interno, aprovado pela Portaria CGU nº 1.028, de 22 de abril de 2015,

Considerando que:

a) O art. 1º do Anexo I do Decreto nº 11.330, de 1º de janeiro de 2023, nos termos definidos pela Lei nº 14.600, de 19 de junho de 2023, estabelece a CGU como "*... órgão central do Sistema de Gestão de Riscos e Controle Interno do Poder Executivo federal...*", considerando, para além da sua função precípua de orientação normativa e supervisão técnica da atividade de auditoria interna governamental, o "X - suporte à gestão de riscos";

b) O Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo federal, aprovado pela Instrução Normativa SFC nº 3, de 9 de junho de 2017, estabelece que "*7. A estrutura de controles internos dos órgãos e entidades da Administração Pública Federal deve contemplar as três linhas de defesa da gestão ou camadas, a qual deve comunicar, de maneira clara, as responsabilidades de todos os envolvidos, provendo uma atuação coordenada e eficiente, sem sobreposições ou lacunas*";

c) O Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo federal, aprovado pela Instrução Normativa SFC nº 3, de 9 de junho de 2017, estabelece para as Unidades de Auditoria Interna Governamental (UAIG) que "*16. As UAIG devem apoiar os órgãos e as entidades do Poder Executivo Federal na estruturação e efetivo fun-*

cionamento da primeira e da segunda linha de defesa da gestão, por meio da prestação de serviços de consultoria e avaliação dos processos de governança, gerenciamento de riscos e controles internos";

d) O Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo federal, aprovado pela Instrução Normativa SFC nº 3, de 9 de junho de 2017, estabelece que "*13. Os Assessores e Assessorias Especiais de Controle Interno (AECI) nos Ministérios integram a segunda linha de defesa e podem ter sua atuação complementada por outras estruturas específicas definidas pelas próprias organizações*"; e

e) O Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo federal, aprovado pela Instrução Normativa SFC nº 3, de 9 de junho de 2017, estabelece que as instâncias da segunda linha devem "*12... apoiar o desenvolvimento dos controles internos da gestão e realizar atividades de supervisão e de monitoramento das atividades desenvolvidas no âmbito da primeira linha de defesa, que incluem gerenciamento de riscos, conformidade, verificação de qualidade, controle financeiro, orientação e treinamento*".

Resolve:

Compete à CGU, enquanto órgão central do Sistema de Gestão de Riscos e Controle Interno do Poder Executivo federal:

a) fornecer orientação normativa e supervisão técnica às UAIG com vistas a uniformizar e qualificar sua atuação como instância de assessoramento e avaliação dos processos de gestão de riscos e controles internos executados no âmbito da unidade auditada; e

b) expedir normas, orientações técnicas e metodologias com vistas a suportar as atividades de gestão de riscos e controles internos desenvolvidas no âmbito da primeira e da segunda linha dos órgãos e entidades do Poder Executivo federal.

As Unidades de Auditoria Interna, no contexto de sua atuação como instância posicionada na terceira linha, devem:

a) apoiar a Unidade Auditada na estruturação e efetivo funcionamento da primeira e da segunda linha, no que se refere aos processos de gestão de riscos e de controles internos; e

b) fornecer serviços de avaliação e de consultoria, segundo os pressupostos de independência e de objetividade, com vistas a propiciar asseguração e suporte às atividades de gestão de riscos e controles internos realizadas pelas instancias de primeira e segunda linhas.

As Assessorias Especiais de Controle Interno, no âmbito de sua atuação como instância posicionada na segunda linha, devem:

a) fornecer orientação técnica, apoio e assessoramento em assuntos pertinentes à gestão de riscos e controle interno;

b) exercer a coordenação do processo de gestão de riscos e controle interno, quando não houver estrutura específica, definida pelo ministério, responsável pelo tema; e

c) fomentar cultura organizacional de gestão de riscos e controles internos no âmbito dos órgãos e entidades vinculados.

CONTROLADORIA-GERAL
DA UNIÃO

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO