AVALIAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS DA CONTROLADORIA-GERAL DA UNIÃO

2022

PRESIDÊNCIA DA REPÚBLICA | SECRETARIA-GERAL
SECRETARIA DE CONTROLE INTERNO

PRESIDÊNCIA DA REPÚBLICA
SECRETARIA-GERAL
SECRETARIA DE CONTROLE INTERNO

AVALIAÇÃO DA MATURIDADE DA GESTÃO DE RISCOS DA CONTROLADORIA-GERAL DA UNIÃO

Nº 1274877

CISET
Presidência da República

Missão

Assegurar a adequabilidade e a qualidade dos mecanismos de governança postos em prática para avaliar, direcionar e monitorar a gestão governamental.

Auditoria Interna Governamental

Atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização; deve buscar auxiliar as organizações públicas a realizarem seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

QUAL FOI O TRABALHO REALIZADO PELA CISET/PR?

Avaliar a maturidade da gestão de riscos da Controladoria-Geral da União e identificar aspectos que podem ser aperfeiçoados, mediante avaliação do ambiente, processos e resultados do gerenciamento de risco colocado em prática pela unidade.

Por que a CISET/PR realizou esse trabalho?

A Instrução Normativa SFC/CGU nº 3, de 9 de junho de 2017 estabeleceu competência à Unidade de Auditoria Interna Governamental (UAIG) para avaliar a eficácia e contribuir para a melhoria do processo de gerenciamento de riscos da Unidade Auditada, observando se, nesse processo: a) riscos significativos são identificados e avaliados; b) respostas aos riscos são estabelecidas de forma compatível com o apetite a risco da Unidade Auditada; e c) informações sobre riscos relevantes são coletadas e comunicadas de forma oportuna, permitindo que os responsáveis cumpram com as suas obrigações.

Considerando que a Secretaria de Controle Interno da Presidência da República (CISET/PR) é a unidade de auditoria interna da Controladoria-Geral da União (CGU), conforme Lei nº 13.844, de 18/6/2019, Art. 51, § 9º, o presente trabalho foi idealizado com o intuito de contribuir para a melhoria do processo de gerenciamento de riscos da Unidade Auditada, por meio da avaliação da maturidade da gestão de riscos da CGU, em atendimento ao previsto no Plano Anual de Auditoria da CISET/PR.

Quais as conclusões alcançadas pela CISET/PR?

A análise realizada permitiu indicar alguns temas em que a gestão de riscos pode ser aprimorada:

- dar continuidade às ações de integração da gestão de riscos estratégicos ao planejamento institucional;
- implementar metodologia de gestão de riscos estratégicos;
- fortalecer as ações de monitoramento, de forma a contemplar a totalidade dos riscos processuais identificados;
- desenvolver indicadores e metas que possibilitem a mensuração da eficácia da gestão de riscos na melhoria dos processos de governança e gestão;
- desenvolver indicadores e metas que possibilitem a mensuração da contribuição dos resultados da gestão de riscos para o alcance dos objetivos estratégicos;
- estabelecer nível de maturidade da gestão de riscos desejado.

LISTA DE SIGLAS E ABREVIATURAS

CGI	Comitê de Governança Interna
CGPPR	Comitê Gerencial de Processos, Projetos e Riscos
CGU	Controladoria-Geral da União
CISET/PR	Secretaria de Controle Interno da Presidência da República
CODIN	Coordenação-Geral de Integração e Desenvolvimento Institucional
DIGOV	Diretoria de Governança
EVG	Escola Virtual de Governo
MOT	Manual de Orientações Técnicas da Atividade de Auditoria
PAINT	Plano Anual de Auditoria Interna
PGR	Política de Gestão de Riscos
SFC	Secretaria Federal de Controle Interno
TCU	Tribunal de Contas da União

SUMÁRIO

1. Introdução

1. De acordo com os princípios definidos pela Instrução Normativa SFC/CGU nº 3/2017, a auditoria interna governamental deve ser uma atividade independente que visa auxiliar as organizações públicas a atingirem seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

2. O gerenciamento de riscos, segundo a Instrução Normativa Conjunta MP/CGU n° 1/2016, refere-se a processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização.

3. A condução do gerenciamento dos riscos deve estar descrita, em linhas gerais, na política de gestão de riscos de uma organização, e deve abordar, dentre outros aspectos, os parâmetro para integração da gestão de riscos ao planejamento estratégico; método e periodicidade para identificação, avaliação, tratamento e monitoramentos dos riscos; e método para avaliação do desempenho da gestão de riscos.

4. O desempenho da gestão de riscos e por conseguinte da sua política, é expresso por meio da maturidade dessa gestão. Conforme Manual de Orientações Técnicas da atividade de auditoria interna (MOT), publicado pela Instrução Normativa SFC nº 8/2017, a maturidade da gestão de riscos refere-se ao grau em que a organização se encontra em relação à adoção e à aplicação da abordagem de gestão de riscos. Em outras palavras, a maturidade da gestão de riscos é determinada pela avaliação da formalização do gerenciamento de riscos, da existência de princípios, estrutura e processos de gestão de riscos, bem como da integração desses aos processos de gestão.

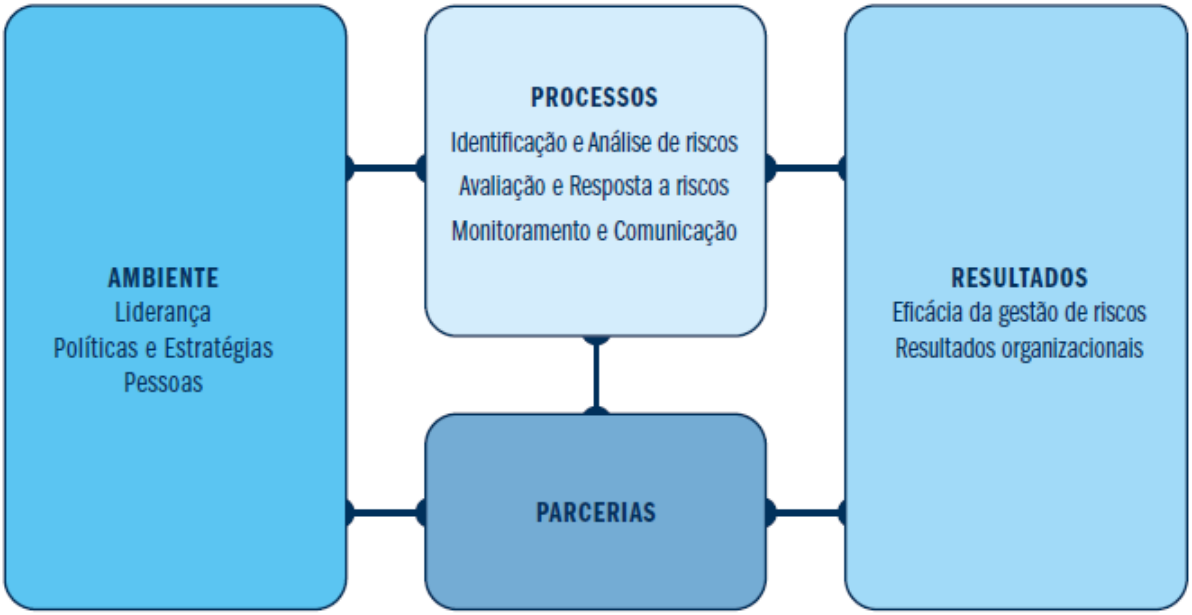
5. Nesse sentido, o presente trabalho, em observância ao previsto no Plano Anual de Auditoria Interna (PAINT) da Secretaria de Controle Interno da Presidência da República (CISET/PR), objetiva avaliar a maturidade da gestão de risco da Controladoria-Geral da União (CGU) e identificar aspectos que podem ser aperfeiçoados, se for o caso, mediante avaliação dos princípios, da estrutura e demais elementos do processo de gerenciamento de riscos colocados em prática pela Unidade Auditada para identificar, analisar, avaliar, tratar e comunicar riscos que possam impactar o alcance dos objetivos e dos resultados da organização.

6. Para tanto, o método adotado baseou-se na Gestão de Riscos – Avaliação da Maturidade, modelo proposto pelo Tribunal de Contas da União (TCU), em 2018. Esse modelo, como descrito na Figura 1, é composto por quatro dimensões e tem como premissas que a maturidade da gestão de riscos é determinada pelas capacidades existentes em termos de liderança, políticas, estratégias e preparo das pessoas para gestão de riscos, somado ao emprego dessas capacidades aos processos e parcerias, os quais se refletem em resultados obtidos na melhoria do desempenho da organização no cumprimento da missão institucional.

7. Neste trabalho, contudo, a avaliação da maturidade da gestão considerou três (ambiente, processos e resultados) das quatro dimensões contidas no modelo original. A exclusão da dimensão “Parcerias” do escopo desta avaliação justifica-se pelo fato de que, segundo modelo original, essa dimensão trata de aspectos relacionados a políticas de gestão

compartilhadas, enquanto que esta avaliação teve por foco a estrutura, os arranjos e as interações exclusivamente internas da organização.

Figura 1 – Modelo de avaliação da maturidade em gestão de riscos



Fonte: Gestão de Riscos – Avaliação da Maturidade, 2018 (TCU).

8. O referido modelo apoia-se em critérios para avaliação da maturidade em gestão de risco. Os critérios propostos, no modelo original, foram adaptados para a avaliação que foi objeto deste Relatório, por meio de questões e subquestões que estão descritas na Tabela 1.

Tabela 1 – Questões e subquestões avaliativas por dimensão

Ambiente	
Questões	Subquestões
1.1. Os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos?	1.1.1. A alta administração e os responsáveis pela governança reconhecem a importância da gestão de riscos, supervisionam a estratégia e exercem suas responsabilidades de governança de riscos.
	1.1.2. Existem estruturas e processos definidos para a governança de riscos e assegura que a gestão de riscos esteja integrada à gestão.
1.2. A organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?	1.2.1. A alta administração/responsáveis pela governança define, comunica, monitora e revisa o apetite a risco.
	1.2.2. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, devidamente vinculada ao planejamento estratégico,

	abordando todos os aspectos relevantes inclusive indicadores de desempenho.
	1.2.3. A administração aloca recursos suficientes e apropriados para a gestão riscos, considerando tamanho e complexidade.
1.3. As pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas para exercê-los?	1.3.1. O pessoal recebe orientação e capacitação suficiente para exercer suas responsabilidades?
	1.3.2. As 1ª e 2ª linhas de defesa têm atuado na estrutura geral de gestão de riscos e controles da organização?
Processos	
Questões	Subquestões
1.4. As atividades de identificação e análise de riscos são aplicadas de forma consistente a todas operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização)?	1.4.1. A identificação de riscos é precedida de uma etapa de estabelecimento do contexto, o qual inclui a respectiva documentação?
	1.4.2. Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos?
1.5. As atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?	1.5.1. Existem critérios estabelecidos para priorização de riscos? Eles estão sendo aplicados?
	1.5.2. A seleção de respostas para tratar riscos considera seu custo-benefício?
	1.5.3. Os responsáveis pelo tratamento de riscos são envolvidos no processo de avaliação e seleção das respostas às ações de tratamento decididas?
	1.5.4. No registro de riscos (sistema, planilhas ou matrizes de avaliação de riscos), a documentação da identificação, análise, avaliação e resposta dos riscos contém elementos suficientes para gerenciamento dos riscos?
1.6. As atividades de monitoramento e comunicação estão estabelecidas e são	1.6.1. Diretrizes e protocolos de informação e comunicação estão estabelecidos e são efetivamente aplicados em todas as fases do processo de gestão de riscos?
	1.6.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado?

aplicadas de forma consistente?	1.6.3. As instâncias de 1ª e 2ª linha de defesa monitoram o alcance de objetivos, riscos e controles chaves?
	1.6.5. São tomadas medidas necessárias para a correção de deficiências e a melhoria contínua do desempenho da gestão de riscos em função dos resultados das atividades de monitoramento?
Resultados	
Questões	Subquestões
1.7. A gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão?	1.7.1. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?
1.8. Os resultados da gestão de riscos têm contribuído para o alcance dos objetivos do órgão?	1.8.1. Qual mecanismo a organização faz uso para verificar que a gestão de riscos está contribuindo para o alcance dos objetivos estratégicos?
	1.8.2. A organização definiu e acompanha o nível de maturidade de gestão de risco que pretende alcançar dentro de um horizonte temporal?

Fonte: Modelo de avaliação da maturidade da gestão de riscos do TCU

9. Cabe destacar que, o modelo de avaliação proposto pelo TCU definiu níveis de maturidade em relação à pontuação alcançada em índice de maturidade apurado em função de análises quantitativas das dimensões avaliadas.

10. Neste trabalho, entretanto, optou-se por avaliar o nível de maturidade da organização por meio de parâmetros qualitativos, identificados no exame dos achados de auditoria, e assim, propor aspectos que possam ser aperfeiçoados pela CGU, no tocante à gestão de riscos.

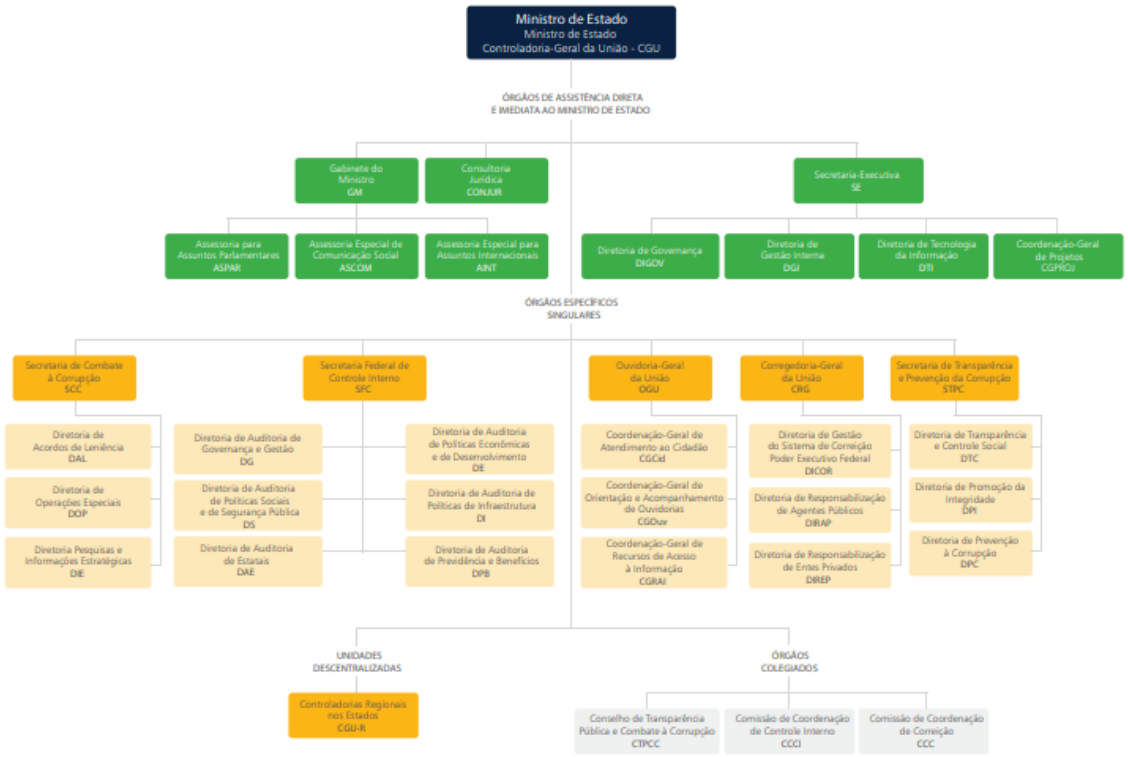
2. Entendimento da Unidade

2.1 Estrutura da CGU

11. A Controladoria-Geral da União (CGU), enquanto integrante da estrutura ministerial do Poder Executivo Federal, conforme Lei nº 13.844/2019, tem competência relacionada aos temas de: defesa do patrimônio público, controle interno, auditoria pública, correição, prevenção e combate à corrupção, atividades de ouvidoria e de transparência da gestão.

12. A estrutura organizacional da CGU, representada na Figura 2 abaixo, de acordo com Decreto n° 11.102/2022, visa atender às suas atribuições como órgão central do Sistema de Controle Interno do Poder Executivo Federal, do Sistema de Correição do Poder Executivo Federal, do Sistema de Ouvidoria do Poder Executivo Federal e do Sistema de Integridade Pública do Poder Executivo Federal.

Figura 2 – Estrutura organizacional da CGU



13. A Figura 3 (página 13) contempla a estrutura organizacional dos órgãos específicos da CGU.

14. No que se refere a riscos, compete à:

A. Diretoria de Governança da Secretaria-Executiva da CGU:

- planejar, coordenar e supervisionar a sistematização, a padronização e a implementação de técnicas e instrumentos de gestão de processos, de projetos e de riscos.

B. Secretaria Federal de Controle - SFC:

- realizar auditorias nos sistemas contábil, financeiro, orçamentário, de pessoal, de tecnologia da informação, de financiamento externo, de cooperação internacional e demais sistemas administrativos e operacionais de órgãos e entidades sob sua jurisdição e propor melhorias e aprimoramentos na gestão de riscos, nos processos de governança e nos controles internos da gestão;
- promover capacitação em temas relacionados às atividades de auditoria interna governamental, governança, gestão de riscos e controles internos.

C. Secretaria de Transparência e Prevenção da Corrupção -STPC:

- promover capacitação e orientação técnica sobre a gestão de riscos nos órgãos e nas entidades da administração pública federal direta, autárquica e fundacional;

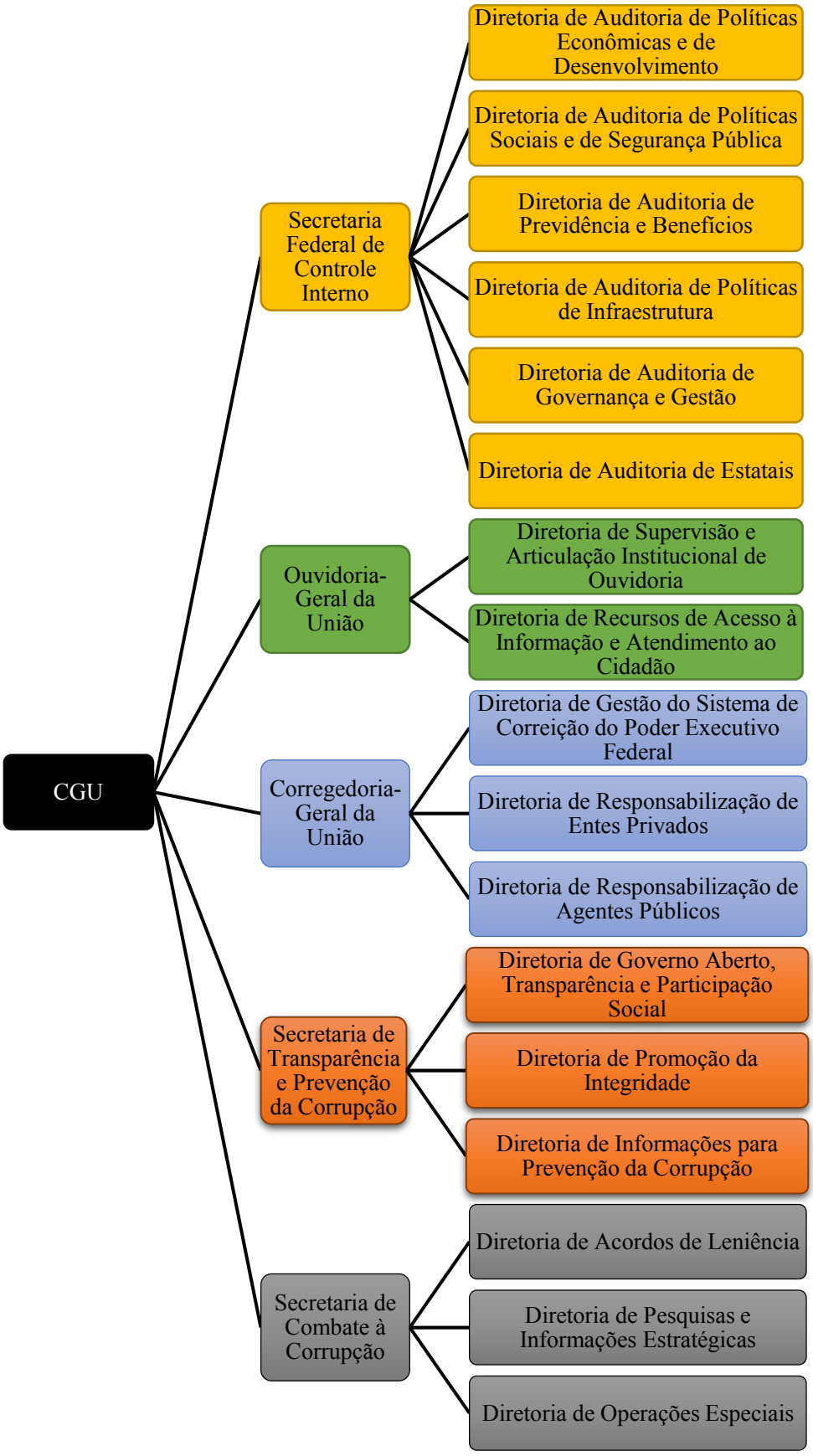
- manifestar-se sobre riscos de conflito de interesses nas consultas submetidas à Controladoria-Geral da União, nos casos de sua competência, e estabelecer medidas para a prevenção ou a eliminação do conflito.

D. Secretaria de Combate à Corrupção- SCC:
- desenvolver estudos, pesquisas e atividades de inteligência de dados sobre temas relacionados com o patrimônio público, a qualidade do gasto público, o mapeamento de riscos no Poder Executivo federal e o combate à fraude e à corrupção.

E. Corregedoria Geral da União – CRG:
- atuar no combate à impunidade na Administração Pública Federal, promovendo, coordenando e acompanhando a execução de ações disciplinares que visem à apuração de responsabilidade administrativa de servidores públicos. Atua também capacitando servidores para composição de comissões disciplinares; realizando seminários com o objetivo de discutir e disseminar as melhores práticas relativas do exercício do Direito Disciplinar; e fortalecendo as unidades componentes do Sistema de Correição do Poder Executivo Federal (SisCOR), exercendo as atividades de órgão central deste sistema.

F. Ouvidoria-Geral da União - OGU
- exercer a supervisão técnica das unidades de ouvidoria do Poder Executivo Federal. Com esse propósito orienta a atuação das unidades de ouvidoria dos órgãos e entidades do Poder Executivo Federal; examina manifestações referentes à prestação de serviços públicos; propõe a adoção de medidas para a correção e a prevenção de falhas e omissões dos responsáveis pela inadequada prestação do serviço público; e contribui com a disseminação das formas de participação popular no acompanhamento e fiscalização da prestação dos serviços públicos.

Figura 3 – Estrutura organizacional dos órgãos específicos da CGU



2.2 Estrutura de governança

15. Segundo Portaria nº 162, de 17/1/2020, publicada em 21/1/2020, a estrutura de governança da CGU é formada por:

- Comitê de Governança Interna – CGI;
- Comitês Gerenciais – CG; e
- Unidades Organizacionais Executivas – UO.

16. O CGI é composto pelos ocupantes dos cargos de: Ministro, Secretário-Executivo, Secretário Federal de Controle Interno, Secretário de Transparência e Prevenção da Corrupção, Secretário de Combate à Corrupção, Corregedor-Geral da União e Ouvidor-Geral da União.

17. Os Comitês Gerenciais são formados por representantes das unidades organizacionais que possuam relação com o respectivo tema estratégico. Essas unidades tem autonomia para propor a criação de CG de acordo com temas estratégicos sob sua responsabilidade e com a participação das áreas relacionadas ao tema.

18. Pelo que se identifica em atos normativos do CGI, os seguintes CG estão instituídos (Tabela 2).

Tabela 2: CG e normativo e data de instituição

Comitê Gerencial de Processos, Projetos e Riscos	**Portaria Normativa nº 8, de 28/4/2022**
Comitê Gerencial de Pesquisa, Conhecimento e Inovação	Portaria Normativa nº 9, de 28/4/2022
Comitê Gerencial de Gestão Orçamentária, Financeira e de Custos	Portaria nº 1.582, de 2/7/2021
Comitê Gerencial de Segurança Corporativa	Portaria nº 947, de 27/4/2021
Comitê Gerencial do Planejamento Estratégico	Portaria nº 1.797, de 7/8/2020
Comitê Gerencial de Contratações	Portaria nº 1.159, de 18/5/2020
Comitê Gerencial de Gestão de Pessoas	Portaria nº 2.870, de 30/8/2019
Comitê Gerencial de Tecnologia da Informação	Portaria nº 1.420, de 16/4/2019

Fonte: CGU – normativos

19. De acordo com Art. 3º da Portaria Normativa nº 8/2022, o Comitê Gerencial de Processos, Projetos e Riscos (CGPPR) é composto por representantes das seguintes unidades:

I - Gabinete do Ministro - GM;

II - Secretaria Federal de Controle Interno - SFC;

III - Secretaria de Transparência e Prevenção da Corrupção - STPC;

IV - Secretaria de Combate à Corrupção - SCC;

V - Corregedoria-Geral da União - CRG;

VI - Ouvidoria-Geral da União - OGU;

VII - Diretoria de Governança - DIGOV;

VIII - Diretoria de Gestão Interna - DGI;

IX - Diretoria de Tecnologia e Informação - DTI; e

X - Controladorias Regionais da União nos Estados.

20. Segundo a citada Portaria, em seu Art 4º, compete ao CGPPR: auxiliar o CGI na execução de suas competências; propor diretrizes, objetivos, iniciativas e indicadores relativos à Gestão de Processos, Projetos, Riscos e à Continuidade de Negócio da CGU; auxiliar o CGI no monitoramento e avaliação da Gestão de Processos, Projetos, Riscos e Continuidade de Negócios; propor a Política de Riscos e Continuidade de Negócio e suas revisões; propor a Metodologia de Gestão de Processos, Projetos e Riscos e suas revisões; propor o Plano de Continuidade de Negócio da CGU e suas revisões; auxiliar o CGI no monitoramento dos riscos e no desempenho das respectivas medidas de controle; auxiliar o CGI no monitoramento do desempenho de processos e projetos; propor os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de Gestão de Riscos, Processos, Projetos e Continuidade de Negócio; e exercer outras atividades definidas pelo CGI.

2.3 Política de Gestão de Risco

21. A Instrução Normativa Conjunta MPOG/CGU nº 1, de 10/05/2016, determina que os órgãos e as entidades do Poder Executivo Federal devem adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança.

22. Nesse sentido a CGU instituiu sua Política de Gestão de Riscos (PGR), por meio da Portaria nº 915/2017, a qual tem por princípios (Art. 3º):

"I - agregar valor e proteger o ambiente interno da CGU;

II - ser parte integrante dos processos organizacionais;

III - subsidiar a tomada de decisões;

IV - abordar explicitamente a incerteza;

V - ser sistemática, estruturada e oportuna;

VI - ser baseada nas melhores informações disponíveis;

VII - considerar fatores humanos e culturais;

VIII - ser transparente e inclusiva;

IX - ser dinâmica, iterativa e capaz de reagir a mudanças;

X - apoiar a melhoria contínua da CGU; e

XI - estar integrada às oportunidades e à inovação."

23. De acordo com Art. 4º, são objetivos da PGR da CGU:

"I - aumentar a probabilidade de atingimento dos objetivos da CGU;

II - fomentar uma gestão proativa;

III - atentar para a necessidade de se identificar e tratar riscos em toda a CGU;

IV - facilitar a identificação de oportunidades e ameaças;

V - prezar pelas conformidades legal e normativa dos processos organizacionais;

VI - melhorar a prestação de contas à sociedade;

VII - melhorar a governança;

VIII - estabelecer uma base confiável para a tomada de decisão e o planejamento;

IX - melhorar o controle interno da gestão;

X - alocar e utilizar eficazmente os recursos para o tratamento de riscos;

XI - melhorar a eficácia e a eficiência operacional;

XII - melhorar a prevenção de perdas e a gestão de incidentes;

XIII - minimizar perdas;

XIV - melhorar a aprendizagem organizacional; e

XV - aumentar a capacidade da organização de se adaptar a mudanças."

24. A citada Portaria orienta que a gestão de riscos:

i) deve estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional; e
ii) sua operacionalização deve ser descrita em metodologia própria, a qual deve contemplar critérios predefinidos de avaliação, de forma a permitir a comparabilidade entre os riscos.

25. Outro aspecto a ser destacado na Instrução Normativa nº 01/2016 é que, de acordo com o Art. 24, a CGU, no cumprimento de suas atribuições institucionais, poderá: avaliar a política de gestão de riscos dos órgãos e entidades do Poder Executivo federal; avaliar se os procedimentos de gestão de riscos estão de acordo com a política de gestão de riscos; e avaliar a eficácia dos controles internos da gestão implementados pelos órgãos e entidades para mitigar os riscos, bem como outras respostas aos riscos avaliados.

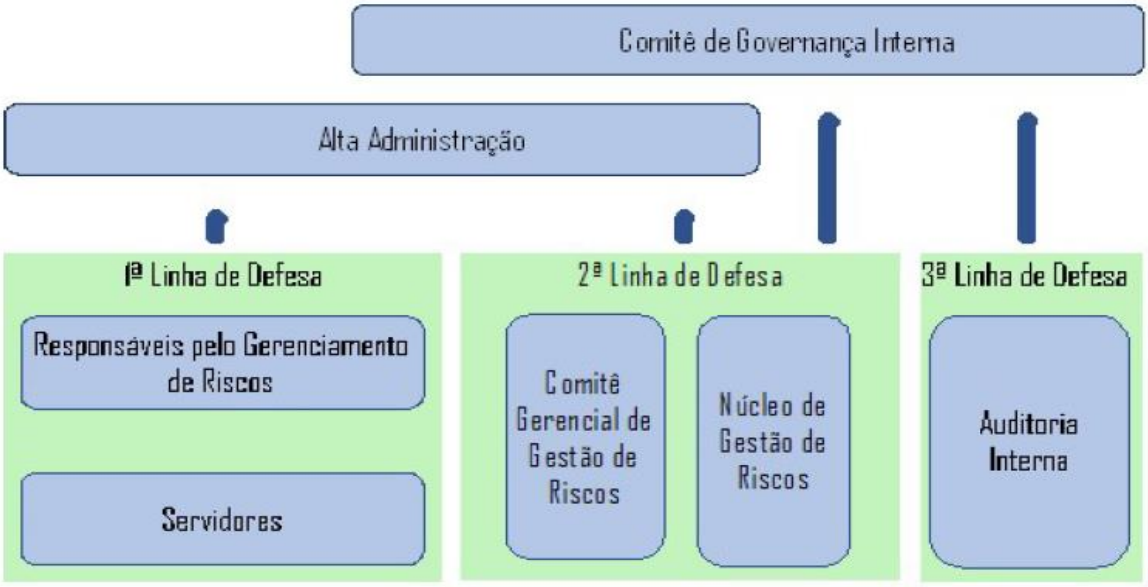
26. A PGR/CGU trouxe competências para o Comitê de Gestão Estratégica, o Comitê Gerencial, o Núcleo de Gestão de Riscos e também para os responsáveis pelo gerenciamento de riscos dos processos organizacionais. Além disso, disciplinou que compete a todos os servidores o monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas, nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

2.4 Metodologia de Gestão de Risco

27. A 2ª versão da Metodologia de Gestão de Riscos da CGU teve por objetivo orientar suas unidades na implementação da gestão de riscos, em conformidade com a PGR/CGU.

28. A Metodologia apresenta os responsáveis pelas três linhas de defesa na gestão de riscos da organização (Figura 4).

Figura 4: Linhas de defesa na gestão de riscos da CGU



29. De acordo com a Metodologia, tanto a primeira quanto a segunda linhas de defesa são exercidas no âmbito da CGU, enquanto que a terceira linha de defesa, de forma singular e em atenção ao parágrafo 9º, Art. 51, da Lei nº 13.844/2019, é exercida pela Secretaria de Controle Interno da Secretaria-Geral da Presidência da República.

30. A citada Metodologia informa que, observando o previsto no Decreto nº 9.203/2017, a Alta Administração da CGU é formada pelos ocupantes dos cargos de Ministro de Estado, Secretário-Executivo, Secretários das unidades finalísticas (Secretaria Federal de Controle Interno, Ouvidoria-Geral da União, Corregedoria-Geral da União, Secretaria de Transparência e Prevenção da Corrupção e Secretaria de Combate à Corrupção, conforme Decreto nº 11.102/2022).

31. A Metodologia, além de informar detalhes sobre a gestão de riscos da CGU apresentados no Manual Operacional de Gestão de Riscos da CGU, contempla o ciclo da gestão de riscos.

32. O Plano de Gestão de Riscos contempla planejamento e realização de trabalhos anteriores à execução da gestão dos riscos, bem como a definição de processos a serem gerenciados, responsáveis pelo processo e cronograma de atividades.

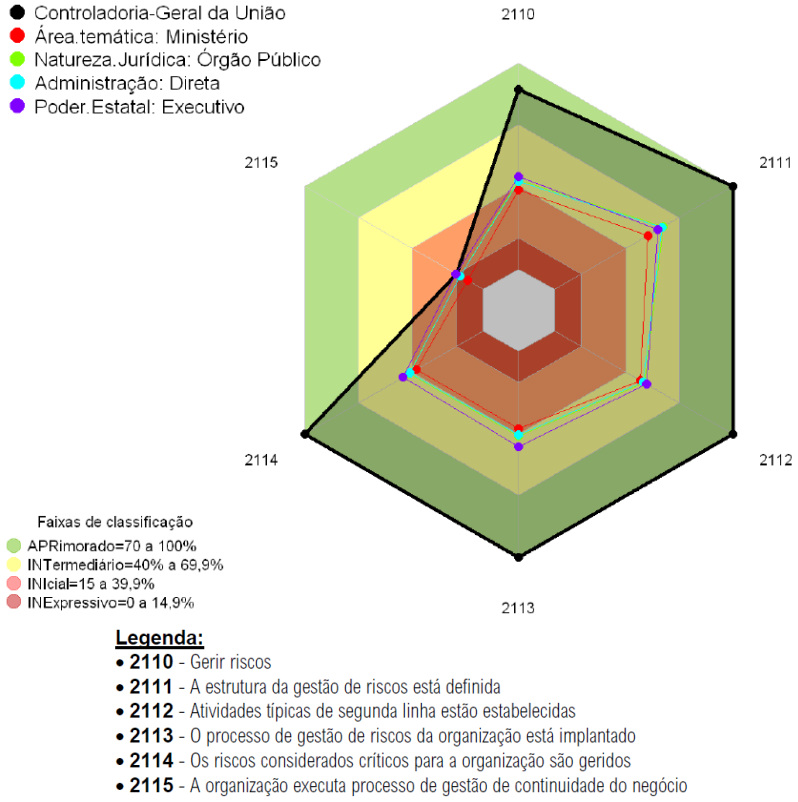
2.5 Índice de Governança e Gestão Públicas

33. O Tribunal de Contas da União (TCU) realiza, sistematicamente, levantamentos para conhecer melhor a situação da governança no setor público e estimular as organizações públicas a adotarem boas práticas de governança.

34. O TCU, por meio do Acórdão nº 2164/2021-Plenário, publicou relatório contendo Levantamento de Governança Pública de 2021, que contou com a participação de 378 organizações públicas, dentre elas a CGU.

35. No que se refere à gestão de riscos, destaca-se o indicador que aborda a Capacidade em gerir riscos (Figura 5) com valor de 87%.

Figura 5 – Indicador - Capacidade em gerir riscos



Legenda:

- **2110** - Gerir riscos
- **2111** - A estrutura da gestão de riscos está definida
- **2112** - Atividades típicas de segunda linha estão estabelecidas
- **2113** - O processo de gestão de riscos da organização está implantado
- **2114** - Os riscos considerados críticos para a organização são geridos
- **2115** - A organização executa processo de gestão de continuidade do negócio

3. Resultado dos Exames

36. Inicialmente, na identificação dos achados fez-se uso: a) das informações e dos esclarecimentos prestados em reuniões realizadas com a unidade auditada, em 22/8/2022 e em 29/11/2022; b) da resposta às duas Solicitações de Auditoria (SA) (e-Aud nº 1288826 e nº 1312177); e c) dos dados dos projetos de gerenciamento de processos e riscos (e-Aud nº 1166434), extraídos do e-Aud, de 3 a 10/10/2022, com verificações pontuais fora desse período.

37. No sistema e-Aud, ao acessar os dados da tarefa 1166434, foram identificados dezesseis processos com riscos gerenciados, dentre os 24 cadastrados, sendo quinze considerados para fins de análise.

38. Quanto aos riscos identificados, ao acessar o e-Aud (1166434), foram apurados o total de 139 riscos nos quinze processos analisados. Logo, os exames realizados estão embasados nesses riscos.

39. Cabe destacar que o mapeamento de processos e riscos é dinâmico. Assim, as informações extraídas no período indicado podem sofrer alterações com o avanço do seu gerenciamento.

40. Para consecução das análises de capacitação e treinamento em gestão de riscos foi utilizada extração dos dados do Plano de Desenvolvimento de Pessoas da CGU apresentada pela unidade.

41. No tocante aos riscos estratégicos, a CGU informou que se encontra em fase de validação interna metodologia para gestão dos riscos estratégicos da organização (proposta anexada na tarefa 1353406). Assim sendo, as análises foram realizadas com base nos riscos processuais.

42. Sobre o assunto, é oportuno consignar que a Controladoria identificou riscos em cerca de 18% dos seus processos / macroprocessos e que está sendo concluída metodologia para identificação e gestão dos riscos estratégicos.

43. Tendo em perspectiva o relato anterior, os resultados dos exames dos achados foram apresentados por dimensão avaliada, como se segue.

DIMENSÃO AMBIENTE

44. Na dimensão Ambiente foram avaliadas as capacidades da organização em termos de liderança, estratégias e capacitação dos servidores, tendo em perspectiva a governança de riscos e a utilização dos riscos na definição da estratégia e dos objetivos organizacionais.

1.1 Os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos?

45. Neste tópico estão contemplados os seguintes aspectos:

- reconhecimento da importância da gestão de riscos;
- supervisão da estratégia e como exercem suas responsabilidades; e
- aderência da gestão de riscos à gestão da unidade.

46. A Controladoria, nos últimos exercícios, passou por várias mudanças institucionais na arquitetura da área responsável pela gestão de riscos. A DIGOV, por meio do Escritório de Riscos e Processos, que integra a Coordenação-Geral de Integração e Desenvolvimento Institucional (CODIN), é atualmente a responsável por exercer formalmente as atribuições de gestão de riscos.

47. Nesse sentido o novo arranjo institucional propiciou uma melhor coordenação e racionalização dos recursos disponíveis entre a Gestão de Processos e a Gestão de Riscos e Governança, favorecendo um avanço no andamento do tema, que pode ser observado pelo exame das atas e pelo progresso das ações.

48. No que se refere às capacitações realizadas sobre gestão de riscos e direcionadas ao corpo interno da CGU, cabe destacar que em 2022, esse número atingiu 96 colaboradores, conforme apresentamos na tabela a seguir.

Tabela 3: Servidores Capacitados em Gestão de Riscos

Ano	Servidores Capacitados
2020	443
2021	88
2022	96
TOTAL	627

49. Dessa forma, constata-se que 31% do total dos servidores da CGU (1984, de acordo com o Relatório de Gestão da CGU - 2021) foram capacitados nesses últimos anos, demonstrando o empenho da entidade para consecução da Política de Gestão Riscos. Destacam-se também os eventos direcionados ao público externo e os disponibilizados na plataforma da Escola Virtual de Governo (EVG).

50. Sobre o acompanhamento da gestão de riscos na CGU, observa–se que a sistemática utilizada para registro, acompanhamento e monitoramento dos dados até 2021 era realizada por meio de planilha eletrônica, o que implicava na possibilidade de perda de informações e outras fragilidades associadas.

51. Todavia, quando da visita da equipe de auditoria, em agosto de 2022, as informações já estavam inseridas no sistema e-Aud. Essa ferramenta permite a automatização dos trabalhos e um melhor acompanhamento e monitoramento das ações, bem como propicia a integração das informações e a comunicação entre as diferentes unidades da CGU.

52. Sobre as dificuldades observadas tanto no monitoramento dos riscos processuais quanto na sua integração ao planejamento estratégico, observamos que os riscos processuais no sistema e-Aud possuem uma vinculação aos objetivos estratégicos, que será utilizada de forma mais efetiva no novo painel em Business Intelligence (BI), conforme informação da CGU.

53. Além disso, a Controladoria destacou que a referida integração deverá ocorrer de forma mais efetiva, quando for revisto o Planejamento Estratégico no exercício de 2023, que abrangerá o período de 2024/2028.

54. No que se refere aos gestão de riscos estratégicos, uma vez que a metodologia encontra-se em processo de validação, a análise quanto à integração se torna inviável neste momento.

55. Desse modo, conclui-se que nos dois últimos exercícios a Política de Gestão de Riscos teve um avanço, especialmente após a implementação da nova arquitetura institucional.

56. Destacam-se também as iniciativas de capacitação, tanto internas quanto externas, bem como os cursos disponibilizados na EVG, o que leva a concluir que tais iniciativas

demonstram o comprometimento da CGU com os objetivos relacionados a este aspecto da Política de Gestão de Riscos.

57. Destarte, em que pese o reposicionamento organizacional, o avanço do mapeamento de processos e riscos e a criação do CGPPR, bem como as iniciativas destacadas nos parágrafos 52; 53 e 54, o quadro atual permite concluir que a gestão de riscos ainda não está totalmente integrada ao Planejamento Estratégico da CGU.

1.2. A organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?

58. Neste tópico estão contemplados os seguintes aspectos:

- a alta administração/responsáveis pela governança define, comunica, monitora e revisa o apetite a risco;
- a organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, devidamente vinculada ao planejamento estratégico, abordando todos os aspectos relevantes inclusive indicadores de desempenho; e
- a administração aloca recursos suficientes e apropriados para a gestão riscos, considerando tamanho e complexidade.

59. No tocante ao apetite a risco, em resposta à SA01, a unidade auditada explicou que esse parâmetro está estabelecido no documento Metodologia de Gestão de Riscos da CGU, o qual definiu um apetite padrão que é usado na obrigatoriedade de tratamento dos riscos.

60. A referida metodologia objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da gestão de riscos na CGU, por meio da definição de um processo de gerenciamento de riscos.

61. Na operacionalização, a gestão de riscos é orientada a processo organizacional e obedece a modelo de aplicação que está integrado à gestão de processos. Por meio desse modelo são priorizados os processos selecionados para serem gerenciados pelo Escritório de Processos e Riscos da CGU. Processos não selecionados podem ter seus riscos gerenciados, desde que obedecida a metodologia e disponibilizado o resultado final ao mencionado Escritório.

62. No referido modelo, após o cálculo dos valores dos níveis de riscos, deve ser considerada a faixa de classificação do risco para a definição da atitude da unidade em relação à priorização para tratamento.

63. A Tabela 4, constante no citado documento, mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções (apetite ao risco).

Tabela 4: Atitude perante o risco para cada classificação

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela

	mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto do Cálculo do Nível de Risco Organizacional (seção 4.10), comunicado ao Comitê de Governança Interna e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Governança Interna.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Comitê de Governança Interna.

Fonte: Metodologia de Gestão de Riscos - CGU

64. Cabe ressaltar que, segundo a metodologia, a unidade organizacional pode definir, em conformidade com o contexto do processo organizacional em avaliação, faixas de classificação distintas das apontadas na Tabela 4, de modo a refletir o nível de apetite a risco desse processo.

65. Considerando que, de acordo com Metodologia de Gestão de Riscos da CGU, o apetite a risco é o "nível de risco que a unidade está disposta a aceitar", o qual deve ser aprovado pelo CGI, além de ser estabelecido no início do processo de gerenciamento de riscos. Uma vez definido o apetite a risco, a unidade declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada; e
- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

66. Nesse sentido, cada risco deve ser relacionado a uma opção de tratamento, a qual depende do nível do risco, do contexto ou do custo do controle, conforme apresentado na Tabela 5.

Tabela 5: Opções de tratamento do risco

Opção de Tratamento Descrição	Descrição
Mitigar	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na CGU, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Na CGU, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a CGU. Na CGU, evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Governança Interna.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Metodologia de Gestão de Riscos - CGU

67. Com relação à comunicação do apetite ao risco, conforme a metodologia, as informações produzidas durante as etapas do processo de gerenciamento de riscos têm caráter restrito. Esse nível de restrição deve ser observado pelos servidores da CGU e demais partes, enquanto que as comunicações gerais sobre gestão de riscos da CGU serão realizadas por meio da IntraCGU e da página da CGU na internet, entre outras formas.

68. Quanto ao monitoramento do apetite ao risco, cabe consignar que, de acordo com resposta à SA02, não obstante a Metodologia de Gestão de Riscos estabeleça o apetite a risco, nos trabalhos realizados de gerenciamentos de processos e riscos, todos os riscos identificados estão sendo considerados para acompanhamento e monitoramento.

69. Convém assinalar que, citando a resposta à SA02, os riscos que extrapolam o apetite a risco estão identificados no sistema e-Aud, sendo que o novo painel em BI, que se encontra na primeira versão e em testes, apresenta de forma gráfica e gerencial a avaliação processual de todos os riscos, especialmente aqueles que estão fora do apetite a risco.

70. De acordo com resposta à SA02, todos os riscos que estão fora do apetite a risco são tratados com a elaboração e implementação de plano de ação pactuado com o Escritório de Processos e Riscos, enquanto que riscos classificados dentro do apetite a risco podem também

possuir plano de ação a depender de avaliação e decisão da unidade responsável pelo processo.

71. Por fim, ao considerar o método de revisão do apetite a risco definido para os processos com os principais riscos organizacionais, na resposta à SA01, consta esclarecimento que a CGU se utiliza da estrutura de governança interna para adotar as decisões táticas que impactam no direcionamento estratégico institucional.

72. O Escritório de Processos e Riscos, valendo-se da interlocução com os membros do CGPPR, solicita a atualização dos dados dos riscos que serão consolidados em painéis. Posteriormente, esses riscos são avaliados pelo Escritório que poderá propor medidas de reavaliação que são levadas, então, à apreciação do Comitê (CGPPR) e, em seguida, ao CGI, nível mais alto de governança interna, para validação ou acréscimo de outras ações.

73. Como já mencionado, no momento, a Metodologia de Gestão de Riscos define um apetite padrão, que é usado na obrigatoriedade de tratamento dos riscos. Caso o responsável pelo processo de negócio entenda que o apetite daquele processo é diferenciado ele pode, desde que justificado e com a validação das instâncias necessárias (conforme metodologia), ter uma postura mais conservadora ou mais arrojada na definição desse apetite específico do seu processo.

74. Com respeito à compatibilização da gestão de riscos ao planejamento estratégico, o Órgão assinalou que o sistema e-Aud permite realizar a vinculação de todos os gerenciamentos de processos e riscos realizados aos artefatos estratégicos da CGU, seja a Cadeia de Valor, seja ao Mapa Estratégico vigente.

75. Apontou ainda que a expectativa para os próximos meses é realizar o monitoramento e a avaliação da gestão de riscos de forma mais efetiva a partir da construção do novo Painel de Processos e Riscos (BI), instrumento que já se encontrava em desenvolvimento, com perspectiva de finalização no segundo semestre de 2022.

76. Além disso, as informações dos riscos já mapeados serão utilizadas no novo ciclo do Planejamento Estratégico 2024-2027, que será construído durante o exercício de 2023. Segundo informação da unidade auditada, há também a perspectiva de avançar nas discussões dos riscos estratégicos, iniciativa que começou no ano de 2021 e que deverá ser retomada no segundo semestre de 2022, conforme pauta já apresentada na primeira reunião do CGPPR, que ocorreu em julho de 2022.

77. É oportuno registrar que essa equipe de auditoria examinou a ata da primeira reunião do CGPPR, acima citada, e verificou que naquela ocasião foi realmente retomada a discussão sobre como deve ser realizado o tratamento dos riscos estratégicos e a seleção de novos processos da Cadeia de Valor a serem gerenciados no segundo semestre de 2022.

78. O mencionado Comitê atua como um colegiado de nível tático que aborda a temática de riscos na unidade. Segundo a CGU, o Escritório de Processos e Riscos, valendo-se da interlocução com os membros do CGPPR coordena as discussões de gestão de riscos, com posterior encaminhamentos ao CGI, nível mais alto de governança interna, para avaliação e aprovação.

79. Ressalte-se enfim que, conforme informação da unidade auditada, são utilizados indicadores para mensurar a maturidade da gestão de riscos, sendo dois indicadores

estratégicos (Indicador Geral de Governança Adaptado ao Poder Executivo Federal; e Abrangência da gestão de riscos).

80. Cabe destacar que os indicadores apresentados para mensuração da maturidade da gestão de riscos serão avaliados na dimensão Resultado deste relatório.

81. Sobre os recursos alocados para ações de gestão de risco nos três últimos exercícios (2020 a 2022), a unidade relatou, sobre a questão tecnológica, que são usados atualmente os recursos do sistema e-Aud.

82. Tal afirmação foi comprovada por essa equipe de auditoria, uma vez que tivemos acesso ao referido sistema e observou-se que a tarefa está cadastrada com o ID 1166434 - Projetos de Gerenciamento de Processos e Riscos da CODIN.

83. Relativamente aos recursos humanos no Escritório de Processos e Riscos, a CGU registrou o exposto na tabela a seguir.

Tabela 6: Recursos humanos dedicados ao tema de gestão de riscos

Ano	Pessoal	Infraestrutura	Tecnológico
2020	1 chefe 4 servidores	• Núcleo de Gestão de Riscos e Integridade (NGRI/GABMIN)	Painel Qlickview Painel do PO Planilha SGP (Excel)
2021	1 chefe 4 servidores	• Núcleo de Gestão de Riscos e Integridade (NGRI/GABMIN) • Comitê Gerencial de Gestão de Riscos e Programa de Integridade	Painel Qlickview Painel do PO Planilha SGP (Excel)
2022	1 chefe, com 3 servidores no primeiro semestre, com aumento de 2 servidores no segundo semestre, a partir do novo concurso da CGU	• Coordenação-Geral de Integração e Desenvolvimento Institucional da Diretoria de Governança (CODIN/DIGOV/SE) • Comitê Gerencial de Processos, Projetos e Riscos (CGGPR)	Painel Qlickview Painel do PO Planilha SGP (Excel) Sistema e-Aud Painéis em PowerBI (em desenvolvimento)

84. Ante isso, verifica-se que o Núcleo de Riscos não sofreu, de forma geral, grandes variações na sua equipe durante o período abordado, uma vez que tinha cinco servidores em 2020, incluindo o Chefe, e espera contar com seis servidores neste semestre, a partir do novo concurso da CGU.

85. Outrossim, deve-se destacar que, além da equipe dedicada à gestão de riscos acima citada, a unidade informou que há alocação de servidores das unidades envolvidas no gerenciamento dos processos, que mais de cinquenta servidores de todas as secretarias do órgão participaram das oficinas de gestão de processos e riscos entre 2020 e 2022 e que ocorre a alocação de pessoal das instâncias de governança (CGPPR e CGI), em momentos específicos.

86. Em relação à gestão de recursos humanos da CGU, ao analisar a Nota Técnica nº 162/2022/DIGOV/SE, observou-se pelo indicador 31 - Taxa de Recursos Humanos da CGU, que avalia o percentual de servidores e empregados públicos em exercício no órgão em relação à necessidade de recursos humanos para o cumprimento de sua missão institucional, a redução sistemática do número de servidores públicos em exercício na Controladoria.

87. A referida Nota destaca também, por meio do Indicador 34 - Abrangência da Gestão de Riscos, que trata da Implementação do Gerenciamento de Riscos nos Processos Organizacionais, o não alcance da meta estabelecida, uma vez que houve suspensão de novos gerenciamentos, a fim de priorizar a implementação do Programa de Gestão de Demandas (PGD) no sistema e-Aud, trabalho esse que demandou grande parte da capacidade operacional da equipe envolvida para estruturar os processos de trabalho nos Planos Operacionais das unidades.

88. Ainda segundo a Nota, outro fator que contribuiu para o não atingimento da meta foi a falta de capacidade operacional das unidades responsáveis pelos processos, considerando outras demandas prioritárias da CGU.

89. Ante o exposto, entende-se que o atual número de servidores no Escritório e principalmente nas unidades da CGU pode representar uma dificuldade para a consecução das atribuições previstas.

90. Ademais, cabe lembrar que o papel da CGU é fundamental para o avanço da Política de Gestão de Riscos em todo o Poder Executivo Federal, tanto pela sua responsabilidade de avaliação, previsto no art. 24 da IN MP/CGU nº 1/2016, como no de assessoramento na execução da Política.

91. Conclui-se assim que:

- o apetite a risco é definido, comunicado internamente, monitorado e revisado;
- a gestão de risco carece de integração ao planejamento estratégico, apesar dos esforços direcionados nesse sentido com o desenvolvimento do e-Aud, do painel BI e da metodologia de riscos estratégicos que está em validação; e
- no tocante à alocação de recursos, em que pese o desenvolvimento de ferramentas tecnológicas (e-Aud e painel BI), a quantidade de servidores envolvidos na gestão de riscos e processos pode se constituir em dificuldade à consecução das atribuições previstas e da difusão interna e externa do referido processo.

1.3. As pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas para exercê-los?

92. Neste tópico estão contemplados os seguintes aspectos:

- o pessoal recebe orientação e capacitação suficiente para exercer suas responsabilidades; e
- as 1ª e 2ª linhas de defesa têm atuado na estrutura geral de gestão de riscos e controles da organização.

93. No que se refere aos aspectos ligados à capacitação, a unidade apresentou o indicador denominado Avaliação da Percepção sobre o Gerenciamento de Processos e Riscos (Aplicação de questionário para avaliação de percepção dos clientes sobre o gerenciamento de processos; o questionário aborda, dentre outros temas, a capacitação), cujas metas e resultados estão apresentados na tabela a seguir.

Tabela 7: Avaliação da Percepção sobre o Gerenciamento de Processos e Riscos

ANO	META	RESULTADOS
2020	0,60	0,84
2021	0,65	0,78
2022	0,70	0,95

94. Como se observa, os resultados superam as metas estabelecidas. Dessa forma, conclui-se que os participantes avaliaram, de forma geral, as capacitações como adequadas.

95. Outra análise realizada pela equipe de auditoria diz respeito às informações disponíveis no sistema informatizado e-Aud, quanto à existência de treinamentos para adequar as pessoas às funções a serem exercidas. Nos quinze processos de riscos mapeados e examinados, em nove consta a informação de que houve treinamento para adequar as pessoas às funções que executam. Além disso, nos seis processos restantes que apontam ausência de treinamento, na metade deles (3) consta informação sobre a existência de plano para enfrentamento desse problema.

96. Sobre o assunto, a unidade esclareceu que os treinamentos citados estão relacionados à execução do processo e não à gestão de riscos e que todos os servidores envolvidos na gestão de riscos são capacitados durante a operacionalização dessa tarefa.

97. Por meio desse esclarecimento entende-se que a integração da gestão de riscos à gestão de processo ainda tem espaço para aprimoramento e que não foi encaminhado documento comprobatório sobre capacitação para todos os operadores da gestão de riscos processuais.

98. No que se refere à atuação da 1ª e 2ª linhas de defesa observa-se que elas efetivamente têm participado da gestão de riscos da unidade. Esse fato é confirmado pela clara definição dos papéis das linhas de defesa, pela normatização da Política de Gestão de Riscos e pelas capacitações realizadas, bem como pela introdução da plataforma e-Aud, que propiciou um ganho na conexão e automatização dos processos internos, e participação das áreas.

DIMENSÃO PROCESSOS

99. Na dimensão Processos foram examinados os processos de gestão de riscos definidos pela organização, considerando a disponibilização de modelo formal, com padrões e critérios definidos para identificação, análise e avaliação de riscos; a seleção e a implementação de respostas aos riscos avaliados; o monitoramento de riscos e controles; e a comunicação sobre riscos entre as partes interessadas.

100. Previamente ao exame dos achados cabe destacar que, dos 91 macroprocessos descritos na Cadeia de Valor, vinte são finalísticos, 33 são gerenciais e 38 de suporte, segundo Relatório de Gestão – 2021 da CGU.

101. Desse total, no período de extração dos dados, dezesseis processos (cerca de 18%) são gerenciados pela Controladoria. A Tabela 8 apresenta o quantitativo de processos gerenciados e com riscos identificados, em relação ao tipo, conforme e-Aud (1166434).

Tabela 8: Processos gerenciados por tipo

Tipo de processo	Quantidade de processos gerenciados	Processo
Finalístico	6	Gerenciar o Direito de Acesso à Informação
		Gerenciar Apuração de Responsabilidade de Entes Privados
		Monitorar Informações de Transparência Pública
		Alavancar Resultados de Acordos de Leniência
		Gerenciar Auditorias Governamentais
		Gerenciar Acordos de Leniência
Gerencial	8	Produzir a Revista CGU
		Gerenciar Manifestações de Ouvidoria
		Gerenciar o Acesso à Informação
		Gerenciar Processos de Negócio
		Gerenciar a Segurança da Informação e Comunicações
		Gerenciar Riscos Corporativos
		Gerenciar Consultas e Pedidos de Autorização sobre Conflito de Interesses
		Elaborar Relatório de Gestão
De suporte	2	Desenvolver Sistemas
		Desenvolver Pessoas (Pós-graduação - afastamento integral, Licença Capacitação e Cursos de curta e média duração)

102. Conforme reposta à SA02, dezoito riscos, cerca de 13% (em relação aos 139 riscos identificados) extrapolaram o apetite ao risco e, de acordo com Metodologia de Gestão de Riscos, devem obrigatoriamente ser tratados e acompanhados.

103. Considerando o relato anterior, o exame dos achados foi apresentado em função das questões de auditoria.

1.4. As atividades de identificação e análise de riscos são aplicadas de forma consistente a todas as operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização)?

104. O objetivo da análise foi verificar a aplicação das atividades de identificação e análise de riscos às operações, funções e atividades relevantes para a realização dos objetivos estratégicos da organização.

105. Para cumprir esse objetivo, a análise foi dividida em duas verificações que versaram sobre: (i) consideração do contexto antes da identificação dos riscos; (ii) envolvimento de pessoas e utilização de técnicas e ferramentas na identificação e análise dos riscos, em quantidade que possibilite a avaliação consistente desses riscos e, por conseguinte, o alcance das metas da organização.

106. Com relação ao contexto (i), os quinze processos com riscos analisados tiveram o cenário elaborado.

107. Pelos dados do e-Aud, entende-se que os cenários analisados colaboraram na identificação e na consolidação inicial dos riscos processuais.

108. Entretanto, alterações no cenário não sugerem a revisão dos riscos. Tal afirmação decorre da resposta à SA01, por meio da qual se informa que o portfólio dos riscos somente é revisado em duas situações: a) no momento em que o responsável pelo processo é instado (pelas instâncias de governança) a reavaliar / atualizar os riscos (classificação, causas, consequências e controles), como se verifca nas atas (6/7/2022 e 20/10/2022) do CGPPR; b) com o monitoramento da ocorrência dos riscos (presença no monitoramento, frequência, medidas para reduzir probabilidade de ocorrência e impacto).

109. Em outro momento, a unidade auditada acrescentou que “os riscos podem ser revisados a qualquer momento pelos responsáveis pelos processos”.

110. No tocante ao envolvimento de pessoas (ii.1) e à utilização de técnicas e ferramentas (ii.2) em quantidade que possibilite a avaliação dos riscos, o exame foi dividido em relação aos dois parâmetros citados.

111. Quanto ao envolvimento de pessoas em quantidade suficiente para avaliação dos riscos (ii.1), para cada processo mapeado consta informação sobre a suficiência dos recursos humanos para a execução do processo. Considerando que a execução do processo engloba a atividade de gestão dos riscos associados, para quinze dos dezesseis processos gerenciados e analisados, oito (53,3%) informaram que os recursos humanos existentes não são suficientes para a execução do processo, conforme informação extraída do e-Aud.

112. Sobre o assunto, a unidade auditada esclareceu que existe diferença entre a quantidade de pessoas destinadas à gestão de riscos e a quantidade de pessoas voltadas para gestão do processo; e que a quantificação citada está relacionada à execução do processo, sem levar em conta as atividades para gestão dos riscos desse processo.

113. Por meio desse esclarecimento entende-se que a integração da gestão de riscos à gestão de processo ainda tem espaço para aprimoramento nesse quesito.

114. De outro modo, nas respostas encaminhadas, afirma-se que o gerenciamento de processos está integrado ao de riscos e que o responsável (em regra, o Coordenador-Geral do processo) pelo processo também é o responsável pelo risco associado.

115. Paralelamente, na avaliação quanto à suficiência de pessoal, é possível considerar o indicador estratégico que aborda a abrangência da gestão de risco (quantidade de processos que implementaram o gerenciamento de riscos sobre a quantidade total de processos).

116. Conforme Nota Técnica 162 (anexo IV da resposta à SA02), no ano de 2020, a meta de 10% dos processos com gerenciamento de riscos foi superada; enquanto que a meta de 2021 (30%) não foi alcançada; já para os anos de 2022 e 2023 foi solicitada a redução da meta (2022 de 50% para 21% - 18 processos; 2023 de 75% para 30% - 28 processos).

117. Nessa Nota consta esclarecimento de que a meta para 2021 (30%) não foi alcançada porque houve suspensão de novos gerenciamentos para implementação do Programa de Gestão de Demandas (PGD) no e-Aud, atividade que demandou grande parte da capacidade operacional da equipe envolvida para estruturar os processos de trabalho relacionados ao PGD. Outro fator que contribuiu para o não atingimento da meta foi a falta de capacidade operacional das unidades responsáveis pelos processos, considerando outras demandas prioritárias da CGU.

118. Assim, os motivos apresentados pela unidade auditada para o indicador Abrangência da Gestão de Risco não ter alcançado a meta, em 2021, e de ter as metas revisadas, em 2022 e 2023, sinalizam a dificuldade com pessoal para o tema da gestão de riscos.

119. A unidade informou que a falta de pessoal disponível para participar dos gerenciamentos de processos e riscos e do posterior monitoramento pode ser um fator realmente crítico para a evolução da temática na instituição. Por outro lado, acrescentou que se espera que o recente concurso da CGU (2021/2022) possa mitigar tal situação.

120. Em relação à utilização de técnicas e ferramentas que possibilitem a avaliação dos riscos (ii.2), a unidade auditada conta com Metodologia de Gestão de Risco publicada (Portaria Nº 910, de 3/4/2018) e revisada (2ª versão - 2021), além de módulo específico para gestão de processos e de riscos no e-Aud (1166434), o qual contempla as etapas descritas na Metodologia, exceto pela Comunicação.

121. Em síntese, conclui-se que:

- o contexto foi considerado na identificação dos riscos de todos os processos analisados;
- a quantificação de horas trabalhadas (h/h) na atividade de gestão de riscos não foi suficiente para identificação e análise dos riscos; e
- a unidade auditada conta com Metodologia de Gestão de Riscos e ferramenta tecnológica para registro das atividades de identificação e análise dos riscos.

1.5. As atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?

122. O objetivo da análise foi verificar a aplicação da avaliação e da resposta aos riscos considerados significativos para a organização.

123. Para cumprir esse objetivo, a análise foi dividida em quatro verificações que versaram sobre: (i) estabelecimento de critérios para priorização dos riscos; (ii) consideração do custo-benefício na seleção de respostas para tratamento dos riscos; (iii) envolvimento dos responsáveis pelo tratamento de riscos no processo de avaliação e seleção das respostas a esses riscos; (iv) completude da documentação de registro dos riscos (identificação, análise, avaliação e resposta) para fins de gerenciamentos desses riscos.

124. Ainda sobre a avaliação e a resposta aos riscos identificados, ao adentrar nos riscos dos processos analisados, algumas inconsistências em relação ao preconizado na Metodologia de Gestão de Riscos foram percebidas.

125. Ao considerar que, nos quinze processos analisados foram identificados 139 riscos, dos quais 97 estão vigentes (69,8%) e os demais encontram-se em análise ou em revisão, as inconsistências percebidas estão a seguir listadas, em relação aos riscos vigentes:

- cinquenta e cinco (56,7%) dos riscos não tiveram sua ocorrência monitorada (conforme resposta à SA02, todos os riscos identificados são considerados para acompanhamento e monitoramento);
- para dois (13,4%) dos quinze processos analisados, a comunicação e a troca de informações entre as unidades que executam o processo foi avaliada como inadequada;
- do total de riscos cuja resposta foi evitar / mitigar / compartilhar, para um deles não foi descrita medida de tratamento; e
- dentre os riscos analisados, para um deles a medida de tratamento foi estabelecida sem prévia definição da resposta a ser dada ao risco (evitar / mitigar / compartilhar).

126. Com relação às inconsistências citadas, cabe esclarecer que se tratam daquelas restantes, após ajustes realizados pela unidade auditado, apontados no Relatório Preliminar desta auditoria.

127. Sobre a comunicação e a troca de informação, a unidade auditada esclareceu que o dado está relacionado à execução do processo e não à gestão de riscos.

128. Esse esclarecimento corrobora o entendimento de que a integração da gestão de riscos à gestão de processo tem espaço para aprimoramento também nesse quesito.

129. No que se refere ao (i) estabelecimento de critérios para priorização dos riscos, a Metodologia de Gestão de Riscos da CGU trouxe definição sobre priorização de riscos (etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa de avaliação de riscos).

130. Ainda de acordo com essa Metodologia, todo risco organizacional que não extrapola o apetite a risco do processo pode ser aceito e uma possível priorização para tratamento deve ser justificada; por outro lado, todo risco organizacional fora da faixa de apetite a risco deve ser tratado e monitorado, sendo que uma possível falta de tratamento deve ser justificada.

131. Para analisar a efetiva utilização da etapa de priorização dos riscos (para fins de tratamento), observou-se a informação descrita na resposta à SA02, de que dezoito riscos extrapolaram o apetite a risco.

132. Em análise amostral, para quinze dos dezoito riscos que extrapolaram o apetite a riscos, segundo afirmação da CGU, medidas de tratamento foram descritas para todos eles, assim como plano de ação (melhoria do processo ou tratamento do risco).

133. Em relação a esses quinze riscos, nove (60%) não foram monitorados nenhuma vez, conforme se verificou pelos dados extraídos do e-Aud, o que descumpre o preconizado na Metodologia de Gestão de Riscos.

134. Sobre o tema, a CGU informou que solicitou a atualização dos dados de monitoramento nas duas reuniões realizadas do CGPPR, o que se confirma ao visitar as atas de 6/7/2022 e 20/10/2022.

135. Para além dos dezoito riscos que extrapolaram o apetite a riscos, segundo afirmação da Controladoria, ao considerar os riscos cuja resposta definida foi evitar, mitigar ou compartilhar (conforme dados do e-Aud) e, portanto, podem ser considerados como aqueles que extrapolaram a faixa de apetite a risco, um não teve a medida de tratamento definida (processo Gerenciar Manifestações de Ouvidoria).

136. Quanto à consideração do custo-benefício na seleção de respostas para tratamento dos riscos (ii), ao adentrar nas subtarefas dos processos analisados identifica-se o item Plano de Ação (5W2H), que contempla coluna relacionada ao custo de medida de tratamento a ser implementada (melhoria do processo ou tratamento de riscos).

137. Apesar da presença da coluna relacionada ao custo, somente em três (20%) dos quinze processos analisados, o custo da medida de tratamento foi informado (mesmo que apenas para uma das medidas de tratamento citadas no Plano de Ação).

138. Quanto ao tema, a CGU esclareceu que a diretriz do Escritório de Processos e Riscos é para que a unidade responsável pelo processo preencha a coluna em questão apenas quando a medida de tratamento de risco ou de melhoria de processo envolver gasto de recurso (uma contratação, por exemplo).

139. A coluna "Custo" tem o fim de ajudar a identificar rapidamente quais medidas de tratamento exigirão recursos, de modo a auxiliar na tomada de decisão e na organização orçamentária.

140. Dessa forma, segundo relato da Controladoria, não há erro no fato da coluna "Custo" não estar preenchida. No entanto, conforme conversado na reunião, o órgão optou por incluir o valor R$ 0,00 nas linhas dessa coluna, para evitar dúvidas.

141. Sobre o envolvimento dos responsáveis pelo tratamento de riscos no processo de avaliação e seleção das respostas a esses riscos (iii), cabe repisar a afirmação da unidade auditada de que os responsáveis pelo processo são também os responsáveis pelo risco (identificação, análise, avaliação, priorização, definição de resposta e monitoramento dos riscos da organização).

142. Com relação ao assunto, ao comparar se a unidade responsável pelo processo também é responsável pela medida de tratamento do risco, seria possível estabelecer correspondência entre quem trata o risco e quem avalia / seleciona a resposta ao risco.

143. Assim, nas subtarefas dos processos analisados, verifica-se que esses quinze processos contêm identificação da unidade responsável pelo processo, dos atores envolvidos no processo, do gerente do plano de trabalho, da equipe do Escritório de Processos e Riscos, e das unidades envolvidas no plano de trabalho.

144. Ainda com relação às subtarefas dos processos analisados, identifica-se a presença de coluna, no Plano de Ação, que especifica o responsável pela medida de tratamento.

145. Comparando os dados citados verifica-se que, em nove (64,3%), dos quinze processos analisados, a unidade responsável pelo processo foi citada, ao menos uma vez, no Plano de Ação, como responsável por alguma ação de melhoria de tratamento.

146. Ao considerar que a unidade responsável pelo processo é a unidade que define o tratamento ao risco, pode-se afirmar que, em 64,3% dos casos, a unidade também está envolvida na resposta ao risco.

147. No tocante à documentação de registro dos riscos (identificação, análise, avaliação e resposta) para fins de gerenciamentos dos riscos (iv), segundo informação da unidade auditada em resposta à SA01, no ano de 2022, o gerenciamento integrado de processos e riscos foi totalmente automatizada e projetizado no e-Aud, além do que toda a base de dados foi migrada de planilhas para esse sistema.

148. Inicialmente, cabe dizer que a Metodologia de Gestão de Riscos da CGU contém detalhamento sobre as etapas da gestão de riscos a serem conduzidas no âmbito da unidade. Ao acessar o e-Aud (1166434), verifica-se que as etapas dessa Metodologia estão representadas no sistema, exceto pela Comunicação.

149. Contudo, o e-Aud não apresenta informações gerenciais e estratégicas de pronto uso pelo gestor, ou seja, o e-Aud não que possibilita a visualização dos dados de forma agregada e com ferramenta de comparação gráfica.

150. Sobre isso, na resposta à SA01, a unidade auditada esclareceu que o Escritório de Processos e Riscos tem capacidade para extrair, pontualmente no e-Aud, as informações de riscos para apresentação à Alta Administração e demais instâncias de governança. Além disso, informou que, com a finalização do novo painel em BI, esse trabalho deve ser aperfeiçoado e otimizado.

151. Por todo o exposto, percebe-se que o e-Aud contém campos suficientes para o gerenciamento dos riscos. Contudo, nem todos os campos estão preenchidos e, mesmo se preenchidos, os dados não se encontram no formato para uso imediato pelo gestor do processo ou pela governança.

152. Por fim, conclui-se que:

- critério foi estabelecido para priorização dos riscos a serem tratados;
- a relação custo-benefício está sendo considerada na definição de tratamento;
- cerca de 64% dos responsáveis pelo tratamento a riscos estão envolvidos a seleção de resposta a riscos; e
- o suporte (e-Aud) para registro dos dados de gestão de riscos está em sintonia com a Metodologia de Gestão de Riscos, contudo não possibilita visualização de informações gerenciais e estratégicos de forma agregada, automatizada e que permita a comparação. Esse problema será mitigado com o novo painel do BI, conforme parágrafo 150.

1.6. As atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente?

153. De acordo com a Metodologia de Gestão de Riscos da CGU, o sistema de informação deve envolver o entendimento do contexto, a identificação dos riscos, a identificação e avaliação dos controles, o cálculo do nível de risco processual, o cálculo do nível do risco organizacional, a definição de resposta aos riscos, a validação de resultados, a implementação do plano de ação, a comunicação, o monitoramento e a reavaliação.

154. Ainda em relação à citada Metodologia, cabe mencionar que as etapas de comunicação e de monitoramento, descritas no respectivo item 4.8, é realizado de forma superficial e genérica, com menção apenas à Norma ISSO 31000:2018, sem, contudo, estabelecer uma descrição detalhada dos procedimentos a serem adotados, o que dificulta a implementação de uma sistemática consistente alinhada ao planejamento estratégico da unidade.

155. Quanto aos temas da comunicação e do monitoramento, a Controladoria informou que: i) o Escritório de Processos e Riscos possui manual operacional detalhando como o monitoramento dos riscos deve ser feito; ii) atualmente, a comunicação é realizada pelas instâncias de Governança (CGI e CGPPR) e, de forma dinâmica, por meio de ferramentas tecnológicas (teams, e-mail, intracgu e repositório de conhecimento); e iii) essas etapas foram abordadas de forma mais detalhada em manuais operacionais (guias), por terem frequência maior de revisão do que a metodologia.

156. No âmbito da CGU o sistema de informação para registro de todas as etapas do processo de gerenciamento de riscos é o e-Aud.

157. No sistema e-Aud, na etapa "Analisar Processo", existem questões relacionadas à comunicação e à troca de informações entre as unidades que executam o processo de gestão de risco.

158. Constatamos que para treze dos quinze processos mapeados, a comunicação e troca de informações entre as unidades que executam o processo foi avaliada pela unidade como adequada. A comunicação e a troca de informação foi considerada NÃO adequada em 2 projetos: "Gerenciar o Acesso à Informação" e "Alavancar Resultados de Acordos de Leniência".

159. No tocante ao assunto, a unidade auditada esclareceu que a informação mencionada refere-se especificamente ao processo que está sendo gerenciado e não trata da comunicação e troca de informações entre a unidade responsável e o Escritório de Processos e Riscos.

160. Pelo esclarecimento entende-se que a integração da gestão de riscos à gestão de processo ainda tem espaço para aprimoramento nesse quesito.

161. Em reunião com a unidade, foi informado que a comunicação da equipe compete ao respectivo coordenador-geral, que é responsável pelo processo e pelos riscos relacionados.

162. Ainda a respeito do assunto, em reposta à SA01, a CGU encaminhou cópias de tela de sua intranet que trata especificamente da gestão de riscos, além de cópias de notícias divulgadas na intranet sobre o gerenciamento de riscos e cópia da tela que permite o servidor receber notificações por e-mail relacionadas ao tema gerenciamento de riscos e controles internos (base de conhecimento).

163. Verificamos que as etapas da metodologia estão representadas no sistema e-Aud, exceto com relação à integração ao planejamento estratégico, que se dará com a

implementação do painel Business Inteligence (BI), que se encontra em desenvolvimento, com finalização prevista para o segundo semestre de 2022.

164. No que se refere ao assunto, a Controladoria informou que todos os processos gerenciados e, consequentemente, seus riscos associados estão relacionados a objetivos estratégicos e que essas informações serão utilizadas no próximo exercício para elaboração do novo planejamento estratégico institucional.

165. Ainda segundo relato da CGU, outra iniciativa que está em andamento, conforme Atas do CGPPR, trata da Metodologia de Riscos Estratégicos que está em fase de validação interna.

166. De acordo com resposta prestada à SA01, "o monitoramento e avaliação da gestão de riscos deve ser realizado diretamente no e-Aud pelo Escritório de Processos e Riscos e instâncias de governança".

167. Os responsáveis por cada processo devem acompanhar seus riscos a qualquer tempo, com a inserção das informações diretamente no referido sistema, podendo inclusive adicionar novas medidas em seu Plano de Ação.

168. Conforme resposta prestada à SA02, os resultados do Indicador Estratégico 34 - Abrangência da Gestão de Riscos, para 2020 a 2022 (parcial), estão descritos na tabela abaixo.

Tabela 9: Resultados do indicador

Abrangência da Gestão de Riscos				
Série Histórica	2020	2021	2022	2023
Meta	10	30	21	30
Resultado	10,99	14,28	16,4 (parcial)	

169. Pelos dados apresentados na Tabela 9, uma vez que nem todos os macroprocessos / processos foram mapeados, por consequência nem todos os riscos processuais são conhecidos.

170. A unidade informou que na primeira reunião do Comitê Gerencial de Processos, Projetos e Riscos – CGPPR (julho 2022) foi solicitado a todas as unidades a validação e atualização de todas as informações, inclusive com o monitoramento dos riscos e indicadores dos processos já gerenciados.

171. Verificamos que no sistema e-Aud as ações de melhoria do processo ou tratamento do risco (plano de ação) constam como coluna (ID do projeto de melhoria de processo ou de medida de tratamento de risco no e-Aud). Contudo, nem sempre essa coluna está visível e não foi possível encontrar nenhum dos projetos relacionados ao plano de ação.

172. Sobre o tema, a Controladoria esclareceu que todas as ações previstas no Plano de Ação devem constar no Plano Operacional da unidade responsável pelo processo. Esses planos operacionais são monitorados pelos próprios gestores das unidades responsáveis e, de forma mais ampla, pela DIGOV (Coordenação-Geral responsável pela gestão desses planos) e, de

forma mais específica, pela CODIN/DIGOV, quando envolvem ações de melhoria de processo ou de mitigação de riscos.

173. Com relação aos critérios e sistemática de revisão dos riscos da organização, em referência à SA02, a unidade informou que o portfólio dos riscos é revisado em dois aspectos: no primeiro, entendido como "atualização do risco", o responsável pelo processo, ao qual o risco se encontra associado, deve reavaliar/atualizar os riscos, as causas, consequências e controles; no segundo aspecto, entendido como "monitoramento dos riscos", o responsável deve prestar informações sobre se o risco aconteceu; se sim, quantas vezes aconteceu, e quais foram as medidas adotadas para que a probabilidade de ocorrência diminua, assim como seu impacto.

174. Em 6/7/2022, em sua primeira reunião, o CGPPR solicitou a todas as unidades a validação e atualização de todas as informações, inclusive com o monitoramento dos riscos e indicadores dos processos já gerenciados. Para esta ação, o Escritório de Processos e Riscos elaborou o guia para atualização e monitoramento dos riscos no e-Aud, para auxiliar o trabalho de revisão dos riscos.

175. As reuniões do CGPPR devem ocorrer, no mínimo, a cada 3 meses, em linha com as diretrizes de governança da CGU, conforme Art. 3º da Portaria Normativa nº 8, de 28 de abril de 2022.

176. Os responsáveis por cada processo devem acompanhar seus riscos a qualquer tempo, com a inserção das informações diretamente no sistema e-Aud, podendo inclusive adicionar novas medidas em seu Plano de Ação, conforme Art. 7º da Portaria Normativa nº 8, de 28 de abril de 2022.

177. Com relação aos 91 macroprocessos citados na cadeia de valor, dezesseis macroprocessos / processos tiveram os riscos identificados - cerca de 18%: Produzir a Revista CGU; Desenvolver Sistemas; Desenvolver Pessoas; Gerenciar o Direito de Acesso à Informação; Gerenciar Manifestações de Ouvidoria; Gerenciar Apuração de Responsabilidade de Entes Privados; Monitorar Informações de Transparência Pública; Alavancar Resultados de Acordos de Leniência; Gerenciar o Acesso à Informação; Gerenciar Processos de Negócio; Gerenciar a Segurança da Informação e Comunicações; Gerenciar Auditorias Governamentais; Gerenciar Riscos Corporativos; Gerenciar Consultas e Pedidos de Autorização sobre Conflito de Interesses; Elaborar Relatório de Gestão; Gerenciar Acordos de Leniência).

162. Verificamos assim que, à época dos trabalhos de campo: i) a etapa de monitoramento foi realizada parcialmente pois, dos 97 riscos vigentes, 42 (43,3%) foram monitorados ao menos uma vez; ii) a comunicação é realizada pelas instâncias de Governança (CGI e CGPPR) e, de forma dinâmica, por meio de ferramentas tecnológicas (teams, e-mail, intracgu e repositório de conhecimento).

DIMENSÃO RESULTADOS

178. Na dimensão Resultados foram examinados os efeitos práticos de gestão de riscos para a melhoria dos processos de governança e de gestão, além de avaliar em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização.

179. O resultado do exame dos achados foi a seguir apresentado, em função das questões elencadas pela equipe de auditoria.

1.7. A gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão?

180. O objetivo da análise foi verificar a eficácia da gestão de riscos para a melhoria dos processos de gestão e de governança organizacional.

181. Para cumprir esse objetivo, a análise buscou verificar se os principais riscos relacionados a cada objetivo, meta ou resultado chave estão identificados e incorporados ao processo de gerenciamento de riscos.

182. Sobre o assunto, cabe destacar que, de acordo com esclarecimentos prestadas em reunião, a unidade auditada gerencia (processos e riscos associados) cerca de 18% de seus macroprocessos / processos; os riscos processuais estão vinculados a objetivos estratégicos; o planejamento estratégico estará integrado à gestão de riscos estratégicos, que se encontra com metodologia em fase de validação.

183. Com relação à vinculação dos processos a objetivos estratégicos, segundo e-Aud, os quinze processos analisados foram relacionados ao objetivo estratégico "OE 14 - Modernizar a gestão estratégica por meio do fomento às melhores práticas de governança, segurança e comunicação organizacional" e estão sendo acompanhados pelos indicadores "Indicador Geral de Governança adaptado ao Poder Executivo Federal" e "Abrangência da gestão de riscos".

184. Conforme Mapa Estratégico da CGU (2020-2023), o objetivo estratégico "Modernizar a gestão estratégica por meio do fomento às melhores práticas de governança, segurança e comunicação organizacional" está sendo monitorado por meio de quatro indicadores, a saber: Índice Geral de Governança adaptado ao Poder Executivo Federal; Abrangência da Gestão de Riscos; Engajamento e Visualizações nos canais eletrônicos da CGU; e Índice de segurança corporativa da CGU – ISC.

185. Os dois primeiros indicadores citados referem-se à governança e à gestão de riscos, respectivamente. O indicador "Índice Geral de Governança adaptado ao Poder Executivo Federal" avalia os critérios de governança e gestão estratégica (governança, integridade, accountabililty, transparência, gestão de processos e projetos e comunicação e segurança institucional), enquanto que o indicador "Abrangência da Gestão de Riscos" trata do percentual de processos que implementaram o gerenciamento de riscos em relação ao total de processos da organização.

186. De acordo com Nota Técnica nº 162/2022/DIGOV/SE/CGU, o indicador que trata do Índice Geral de Governança demonstrou que as metas para 2020 (19) e 2021 (22) não foram alcançadas (18 e 19, respectivamente) apesar de se aproximarem do resultado esperado.

187. Sobre esse indicador, na citada Nota Técnica consta afirmação que para alcance ou superação das metas desse indicador, para os próximos exercícios, faz-se necessário que a CGU fortaleça a atuação em pontos específicos da governança e gestão estratégica, como, por exemplo: liderança; estrutura interna de governança; promoção da ética e da integridade; gestão de riscos; demandas das partes interessadas; gerenciamento de projetos, gestão de contrações; segurança corporativa; comunicação institucional e relações institucionais.

188. Também de acordo essa Nota Técnica nº 162, o indicador que trata da abrangência da gestão de riscos evidenciou que a meta para 2020 (10%) foi superada (10,99%), enquanto que a meta para 2021 (30%) não foi alcançada (14,28%).

189. Quanto a esse indicador, a referida Nota informa que foi proposta redução das metas estabelecidas para 2022 (de 50% para 21% - 18 processos) e para 2023 (de 75% para 30% - 28 processos).

190. Considerando que os indicadores abordam de forma isolada a evolução da governança e da gestão de riscos (sob certos critérios), o que, em tese, possibilitaria emitir conclusão sobre o processo de governança e de gestão de riscos, eles efetivamente não demonstram diretamente o impacto da gestão de riscos na melhoria dos citados processos.

191. Quanto ao tema, a CGU informou que a demonstração do impacto do trabalho de gerenciamento de processos e riscos poderá ser avaliada no futuro, com o avanço do acompanhamento dos indicadores e das metas pactuados para cada gerenciamento.

192. Além disso, a Controladoria lembrou que realiza pesquisa para avaliar a percepção dos gestores, ao final de cada processo gerenciado, quanto ao valor agregado pela gestão de riscos à gestão de processos e riscos.

193. Dessa forma, entendemos que tal pesquisa poderia ser utilizada na avaliação da eficácia da gestão de risco na melhoria dos processos de governança e gestão, em conjunto com outros parâmetros a serem desenvolvidos pela unidade.

1.8. Os resultados da gestão de riscos têm contribuído para o alcance dos objetivos do órgão?

194. O objetivo da análise foi verificar a contribuição da gestão de riscos para o alcance dos objetivos organizacionais.

195. Para cumprir esse objetivo, a análise foi dividida em duas verificações que versaram sobre: (i) mecanismo usado pela organização para avaliar se a gestão de riscos está contribuindo para o alcance dos objetivos estratégicos; (ii) definição e acompanhamento do nível de maturidade da gestão de riscos almejado, em horizonte temporal.

196. No que se refere ao (i) mecanismo usado para avaliar se a gestão de riscos está contribuindo para o alcance dos objetivos estratégicos, como informado na resposta à SA01, o sistema e-Aud permite realizar a vinculação de todos os processos gerenciados (com riscos identificados) aos artefatos estratégicos da CGU, seja a Cadeia de Valor, seja ao Mapa Estratégico vigente; além disso, as informações dos riscos já mapeados serão utilizadas no novo ciclo do Planejamento Estratégico 2024-2027, que será construído durante o exercício de 2023.

197. Pela resposta encaminhada conclui-se que o processo de gerenciamento de processos e riscos está atrelado aos referenciais estratégicos da organização, mas que a utilização dos dados da gestão de riscos ainda é incipiente, com espaço para avançar na contribuição ao alcance dos objetivos estratégicos.

198. Quanto à (ii) definição e acompanhamento do nível de maturidade da gestão de riscos almejado, conforme afirmação contida na resposta à SA01, a organização faz uso do "Índice

Geral de Governança adaptado ao Poder Executivo Federal" e do indicador "Abrangência da Gestão de Riscos" para mensurar a maturidade da gestão de riscos e sua efetividade.

199. Como visto anteriormente, o primeiro indicador citado avalia os critérios de governança e gestão estratégica (governança, integridade, accountabililty, transparência, gestão de processos e projetos e comunicação e segurança institucional), enquanto que o indicador "Abrangência da Gestão de Riscos" trata do percentual de processos que implementaram o gerenciamento de riscos em relação ao total de processos da organização.

200. Conclui-se que esses indicadores não retratam o nível de maturidade da gestão de riscos da Controladoria e, portanto, não permitem verificar a contribuição dos resultados da gestão de riscos para o alcance dos objetivos da CGU.

4. Recomendações

201. Diante dos achados apresentados no corpo deste Relatório de Auditoria, seguem as recomendações que visam auxiliar o gestor na implementação de melhorias nos processos analisados.

202. Para tanto, a CGU deverá apresentar a esta CISET, no prazo de trinta dias após o recebimento do relatório definitivo, plano de ação, contendo, para cada recomendação indicada a seguir, as medidas a serem adotadas, o prazo para implementação e o responsável pelo desenvolvimento das ações, de modo a solucionar os achados apontados neste relatório, sem prejuízo de outras ações que, de igual modo, contribuam efetivamente para o aperfeiçoamento da gestão.

Dimensão Ambiente

203. Recomendação 1: Dar continuidade às ações de integração da gestão de riscos estratégicos ao planejamento institucional;

204. Recomendação 2: Prosseguir com a implementação de solução tecnológica para extração de informações gerenciais e estratégicas;

Dimensão Processo

205. Recomendação 3: Implementar metodologia de gestão de riscos estratégicos;

206. Recomendação 4: Proceder aos ajustes das inconsistências citadas neste relatório e promover a revisão periódica no registro dos riscos processuais;

207. Recomendação 5: Fortalecer as ações de monitoramento, de forma a contemplar a totalidade dos riscos processuais identificados, conforme estabelecido na Metodologia de Gestão de Riscos;

Dimensão Resultado

208. Recomendação 6: Desenvolver indicadores e metas que possibilitem a mensuração da eficácia da gestão de riscos na melhoria dos processos de governança e gestão;

209. Recomendação 7: Desenvolver indicadores e metas que possibilitem a mensuração da contribuição dos resultados da gestão de riscos para o alcance dos objetivos estratégicos; e

210. Recomendação 8: Estabelecer nível de maturidade da gestão de riscos desejado, com prazo para alcance e metas parciais.

5. Conclusão

211. Diante do exposto, verificou-se que a Controladoria Geral da União avançou na execução da Política de Gestão de Riscos, no período de 2021/2022, entretanto ficou clara a necessidade de progresso em temas como:

- integração da gestão de riscos ao Planejamento Estratégico;
- implementação de ferramenta (solução tecnológica) para extração de dados gerenciais e estratégicos;
- priorização do gerenciamento dos riscos estratégicos;
- aprimoramento do mecanismo de monitoramento dos riscos processuais;
- correção de inconsistência frente à Metodologia de Gestão de Riscos elaborada;
- mensuração da eficácia da gestão de riscos na melhoria dos processos de gestão e de governança;
- definição de indicadores e de metas que possibilitem a mensuração da eficácia da gestão de riscos; e
- estabelecimento do nível de maturidade a ser atingido dentro de um horizonte temporal.

212. Acrescentam-se como temas que poderiam ser considerados para revisão o detalhamento das etapas de monitoramento e de comunicação da Metodologia de Gestão de Riscos, bem como o critério adotado para o estabelecimento de apetite a riscos padrão para todos os processos mapeados.

213. Vale destacar que, durante a execução dos trabalhos foram observadas boas práticas que podem ser replicadas a outras unidades do Governo Federal, dentre elas destacam-se:

- o esforço despendido nas ações de capacitação do corpo funcional, tanto interno quanto externo à CGU, destacando-se os treinamentos disponibilizados em plataforma digital por meio da EVG, cujo alcance é significativo; e
- a modulação do sistema e-Aud, para informatização do registro das ações e tarefas da gestão de riscos, que propiciou melhor integração das informações e comunicação entre as unidades da CGU, bem como permitiu a racionalização das atividades.

214. Por fim entende-se que, para a continuidade das ações de avaliação do nível de maturidade da gestão de riscos, devem ser realizados exames sobre o tema, nos próximos exercícios, inclusive com incorporação da Dimensão “Parcerias”.