

MANUAL DE GESTÃO DE RISCOS DO TCU



República Federativa do Brasil

Tribunal de Contas da União

MINISTROS

Raimundo Carreiro (Presidente)
José Múcio Monteiro (Vice-Presidente)
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Ana Arraes
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva (Procuradora-Geral)
Lucas Rocha Furtado (Subprocurador-Geral)
Paulo Soares Bugarin (Subprocurador-Geral)
Marinus Eduardo de Vries Marsico (Procurador)
Júlio Marcelo de Oliveira (Procurador)
Sérgio Ricardo Costa Caribé (Procurador)
Rodrigo Medeiros de Lima (Procurador)

MANUAL DE GESTÃO DE RISCOS DO TCU

Segepres/Seplan – Brasília, Maio, 2018

TRIBUNAL DE CONTAS DA UNIÃO 

© Copyright 2018, Tribunal de Contas de União
Impresso no Brasil / *Printed in Brazil*
<www.tcu.gov.br>

Permite-se a reprodução desta publicação,
em parte ou no todo, sem alteração do conteúdo,
desde que citada a fonte e sem fins comerciais.

Brasil. Tribunal de Contas da União.

Manual de gestão de riscos do TCU / Tribunal de Contas da União. –
Brasília : TCU, Secretaria de Planejamento, Governança e Gestão
(Seplan), 2018.

46 p. : il.

Inclui glossário com a definição dos principais termos utilizados.

1. Administração pública – governança. 2. Administração pública -
eficiência. 3. Gestão de riscos. 4. Controle interno. I. Título.

MANUAL DE GESTÃO DE RISCOS DO TCU

Segepres/Seplan – Brasília, Maio, 2018

SUMÁRIO

Apresentação	7
1. Introdução	11
2. Objetivo da Gestão de Riscos no TCU	14
3. Princípios da Gestão de Riscos no TCU	15
4. Objetos da Gestão de Riscos	17
5. Processo de Gestão de Riscos	18
5.1 Estabelecimento do Contexto	19
5.2 Identificação dos Riscos	20
5.3 Análise dos Riscos	21
5.4 Avaliação dos Riscos	25
5.5 Tratamento dos Riscos	26
5.6 Monitoramento	29
5.7 Comunicação	30
5.8 Melhoria Contínua	31

6. Sistema de Gestão de Riscos do TCU (SGR/TCU) _____	32
6.1 Instâncias e Responsabilidades _____	32
6.2 Funcionamento do Sistema de Gestão de Riscos _____	36
6.3 Integração da Gestão de Riscos com o Planejamento Estratégico _____	39
6.4 Atuação dos Coordenadores Setoriais de Risco (CSR) _____	40
7. Referências Bibliográficas _____	42
8. Glossário _____	44
9. Anexo _____	46
Tabela de Análise e Avaliação de Risco - Processos de trabalho _	46



APRESENTAÇÃO

O Tribunal de Contas da União, na busca pela excelência no exercício de suas competências, tem adotado estratégias que possibilitem maximizar a efetividade de suas ações.

A sistematização da gestão de riscos em nível institucional constitui estratégia que aumenta a capacidade da organização para lidar com incertezas, estimula a transparência e contribui para o uso eficiente, eficaz e efetivo de recursos, bem como para o fortalecimento da imagem da instituição.

As melhores práticas internacionais de gestão recomendam a adoção de sistemas de gerenciamento de riscos associados aos processos de planejamento, de tomada de decisão e de execução dos trabalhos relevantes, de modo a garantir que as finalidades públicas sejam alcançadas de fato, com a melhor relação custo-benefício.

Apartir de diversas iniciativas deste Tribunal, do Ministério da Transparência e Controladoria-Geral da União (CGU) e do Conselho Nacional de Justiça (CNJ), as práticas de gestão de riscos têm sido gradualmente institucionalizadas na administração pública e, em nível federal, já são até mesmo obrigatórias.

Em abril de 2017, foi aprovada a Resolução-TCU nº 287, oportunidade em que o Plenário definiu a política interna de gestão de riscos da Casa (PGR/TCU), cuja implementação está em andamento, sob a coordenação da Secretaria de Planejamento, Governança e Gestão (Seplan), unidade central de coordenação e supervisão do Sistema de Gestão de Riscos do Tribunal (SGR/TCU).

O presente Manual integra o conjunto de instrumentos essenciais para a construção do SGR/TCU, o qual dará suporte para a concepção, a implementação, o monitoramento e a melhoria contínua da gestão de riscos em todo o Tribunal. Desse modo, este Manual oferece aos gestores orientações específicas para o início da gestão interna de riscos.

Ressalto a necessidade da participação coordenada de toda a Casa, com vistas à adequada gestão de riscos, de modo que eles sejam identificados e seus possíveis impactos devidamente avaliados.

A estratégia escolhida para implantação da gestão de riscos é iterativa. Baseia-se em ciclos sucessivos, com complexidade crescente. Ou seja, estamos começando com processos e produtos simples, experiências-piloto, projetos rápidos e protótipos, procedendo às correções de rumo necessárias, para, posteriormente, avançar no sentido da evolução para modelos mais sofisticados.

Nesse sentido, esta primeira versão do Manual de Gestão de Riscos do TCU reflete essa simplicidade de abordagem e de linguagem. A expectativa é que o Manual constitua valioso instrumento nas mãos dos gestores e servidores do TCU e de seus parceiros públicos e privados, proporcionando orientações para a adequada coordenação das atividades de direção e controle da organização no que se refere a riscos e oportunidades.

Como o sucesso da gestão de riscos depende do envolvimento de todos, conclamo as pessoas que trabalham nesta Casa a se engajarem no desafio de pensar o nosso trabalho pela ótica dos riscos e, portanto, de imprimir a nosso ambiente interno, cada vez mais, o espírito da eficiência, da eficácia, da orientação aos resultados, da cooperação recíproca e da responsabilidade profissional, elementos que a gestão de riscos busca, motiva e induz.

Por fim, de modo a permitir a esperada evolução do modelo de gestão de riscos interna e o aperfeiçoamento deste Manual, solicito que dúvidas, críticas ou sugestões sejam encaminhadas para o endereço eletrônico seplan@tcu.gov.br.

Conto com a colaboração de todos.

RAIMUNDO CARREIRO
Presidente



1. INTRODUÇÃO

A iniciativa de implantar a gestão de riscos no setor público é relativamente recente no Brasil, embora, em alguns países, tenha começado há mais tempo. No Reino Unido, no início dos anos 1990, foi implantada com a finalidade de aumentar o empreendedorismo no setor público e, desde então, vem se consolidando como parte integrante do processo de gestão. Atualmente, a *Commonwealth*¹ conta com uma política de gestão de riscos para o setor público.

No contexto brasileiro, é importante lembrar a Emenda Constitucional nº 19, de 1998, que acrescentou o conceito da eficiência no rol dos princípios que regem toda a administração pública federal (CF, art. 37, *caput*). O objetivo principal da gestão de riscos é aumentar o grau de certeza na consecução dos objetivos, o que tem impacto direto na eficiência.

O Ministério do Planejamento, Desenvolvimento e Gestão (MP), Ministério da Transparência e Controladoria-Geral da União (CGU) expediram, em 2016, a Instrução Normativa Conjunta nº 01, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. O MP lançou, em 2017, o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.

Ainda em 2017, foi editado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, que trata, entre outros temas, da gestão de riscos na administração pública.

¹ Associação de países, integrada pelo Reino Unido e outros países, que foram parte do antigo Império Britânico

O Tribunal de Contas da União (TCU) começou, em 2012, a mapear a situação da gestão de riscos de entidades da administração indireta. Em 2017, essa avaliação abrangeu todas as entidades do setor público no âmbito do Índice Geral de Governança do Setor Público (IGG), incluindo-se aí o TCU.

A Secretaria-Geral de Controle Externo do TCU (Segecex) lançou, em 2017, o **Roteiro de Auditoria de Gestão de Riscos**, com o objetivo de apoiar os auditores do setor público – do controle externo, interno ou das auditorias internas – a avaliar a maturidade da gestão de riscos das organizações públicas e a identificar os aspectos que necessitam ser aperfeiçoados. Para conhecer o roteiro, acesse o endereço: <http://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm>.

Em consonância com princípios da ISSAI 12², o TCU deve liderar pelo exemplo, implantando sua própria gestão de riscos organizacional. Nesse sentido, o Tribunal aprovou, em 2017, a sua Política de Gestão de Riscos³ (PGR/TCU) e vem adotando ações para implementá-la. A Política está disponível no endereço: <http://portal.tcu.gov.br/biblioteca-digital/politica-de-gestao-de-riscos-do-tcu.htm>.

Este manual constitui uma etapa importante nessa direção e tem por objetivo orientar os gestores do TCU na gestão de riscos organizacional do Tribunal, prática que constitui um dos elementos de uma boa governança corporativa.

A proposta do manual é que o gestor possa encontrar, de maneira rápida e simples, tudo o que precisa para compreender o assunto em um só documento. Outros princípios que nortearam a elaboração do manual são os da simplicidade, da facilidade de entendimento e o da objetividade, de modo a espelhar o espírito da gestão de riscos que se pretende para o TCU.

O manual foi elaborado a partir da política de gestão de riscos e representa um instrumento importante para sua implementação.

Em termos de conteúdo, aborda o objetivo e os princípios da gestão de riscos no TCU, sua governança e seu funcionamento, o processo de gestão de riscos propriamente dito e um glossário com a definição dos principais termos utilizados.

2 ISSAI 12: Valor e Benefício das Entidades Fiscalizadoras Superiores – aprovada pela INTOSAI em 2013.

3 Resolução TCU nº 287, de 12 de abril de 2017.



2. OBJETIVO DA GESTÃO DE RISCOS NO TCU

A gestão de riscos no TCU tem como objetivo auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais.

Não considerar explicitamente os riscos na tomada de decisões pode acarretar o não alcance dos objetivos ou resultados que poderiam ser atingidos.

Conceitos Básicos

Risco – possibilidade de que um evento afete negativamente o alcance dos objetivos.

Oportunidade – possibilidade de que um evento afete positivamente o alcance de objetivos.

3. PRINCÍPIOS DA GESTÃO DE RISCOS NO TCU

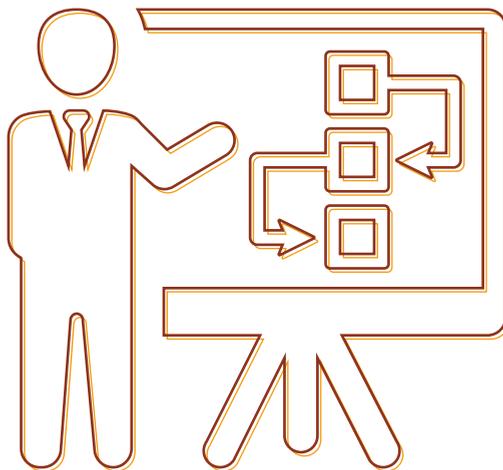
Conforme a Política de Gestão de Riscos do TCU, são os seguintes os princípios que regem a gestão de riscos no TCU.

- **Fomentar a inovação e a ação empreendedora responsáveis**
Ao realizar algo que nunca foi feito antes ou que implique riscos, identificar, avaliar e tratar esses riscos aumenta a chance de sucesso. Mesmo que a iniciativa não tenha sucesso por algum motivo, estará documentado que o gestor tinha consciência dos riscos e adotou as providências necessárias para mitigá-los, o que demonstra uma gestão responsável.
- **Considerar riscos e, também, oportunidades**
A oportunidade é também chamada de risco positivo, pois constitui a possibilidade de um evento afetar positivamente os objetivos. A boa gestão de riscos deve, também, considerar as oportunidades, pois o gestor precisa estar preparado para aproveitá-las.
- **Aplicar-se a qualquer tipo de atividade ou projeto**
A gestão de riscos pode ser aplicada a qualquer ação organizacional que tenha um objetivo claro ou da qual resulte um produto ou serviço definido.
- **Aplicar-se de forma contínua e integrada aos processos de trabalho**
Gerir riscos não pode ser uma atividade esporádica e descasada do dia a dia do trabalho. Deve ser uma atitude permanente, parte integrante do processo decisório, desde que apresente relação custo-benefício favorável.

- **Ser implantada por meio de ciclos de revisão e melhoria contínua**
A implantação da gestão de riscos deve ser um processo gradual e progressivo, com revisões periódicas, a partir de mudanças organizacionais e/ou no ambiente externo e dos resultados das avaliações do funcionamento do sistema de gestão de riscos.
- **Considerar a importância dos fatores humanos e culturais**
A percepção sobre os riscos e seus impactos no alcance dos objetivos depende das características das pessoas responsáveis pela gestão desses riscos e da cultura de determinado órgão ou área da instituição em que esses riscos são avaliados.
Nesse sentido, uma boa gestão de riscos deve considerar a influência dos fatores humanos e da cultura organizacional na identificação, na avaliação e no tratamento dos riscos. O sucesso ou fracasso da gestão de riscos depende da cultura organizacional.
- **Ser dirigida, apoiada e monitorada pela alta administração**
A alta administração tem a responsabilidade de conduzir o processo de implantação, de manter o sistema funcionando com eficiência e economicidade, de gerenciar os riscos-chave para o TCU e liderar pelo exemplo, demonstrando efetivo compromisso com a gestão de riscos.

4. OBJETOS DA GESTÃO DE RISCOS

São objetos da gestão de riscos qualquer **processo de trabalho, atividade, projeto, iniciativa** ou **ação de plano institucional**, assim como os **recursos que dão suporte à realização dos objetivos do TCU. Unidades organizacionais** também podem ser objeto da gestão de riscos.



5. PROCESSO DE GESTÃO DE RISCOS

Para realizar a gestão de riscos de quaisquer objetos, as seguintes etapas devem ser seguidas:

- estabelecimento do contexto;
- identificação dos riscos;
- análise dos riscos;
- avaliação dos riscos;
- tratamento dos riscos;
- comunicação e consulta com partes interessadas;
- monitoramento;
- melhoria contínua.

O processo de gestão de riscos pode ser visualizado na figura abaixo.



Figura 1: Processo de Gestão de Riscos (ISO 31000 – Adaptado)

Dada a natureza multidisciplinar da gestão de riscos, o processo deve ser conduzido, preferencialmente, de forma coletiva, em oficinas de trabalho, por pessoas que conhecem aquele processo, projeto etc.

■ 5.1 ESTABELECIMENTO DO CONTEXTO



Consiste em **compreender o ambiente externo e interno** no qual o objeto de gestão de riscos se encontra inserido e em identificar parâmetros e critérios a serem considerados no processo de gestão de riscos.

O estabelecimento do contexto deve seguir os seguintes passos:

- identificar quais objetivos ou resultados devem ser alcançados;
- identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;
- identificar as pessoas envolvidas nesses processos e especialistas na área;
- mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc.).

■ 5.2 IDENTIFICAÇÃO DOS RISCOS



Compreende o **reconhecimento e a descrição dos riscos** relacionados aos objetivos/resultados de um objeto de gestão de riscos, envolvendo a identificação de possíveis fontes de riscos.

A identificação dos riscos deve seguir os seguintes passos:

- identificar com clareza o(s) objetivo(s)/resultado(s);
- listar, para cada objetivo/resultado, os eventos que possam vir a ter impacto negativo no alcance do objetivo/resultado;
- descrever como cada risco impacta o objetivo/resultado a ele associado.

A identificação dos riscos deve ser realizada em oficinas de trabalho ou, dependendo do objeto, pelo próprio gestor do risco.

No processo de identificação de riscos, deve-se buscar a participação de pessoas que conheçam bem o objeto de gestão de riscos.

Devem ser utilizadas técnicas/ferramentas que permitam a coleta do maior número de riscos, tais como *brainstorming*, *brainwriting*, entrevistas, visitas técnicas, pesquisas etc.

São dicas que facilitam a identificação dos riscos:

- responder à seguinte pergunta-chave: o que pode atrapalhar o alcance do objetivo/resultado?
- considerar os fatores de sucesso para a consecução dos objetivos – qualquer evento que afete o fator de sucesso potencialmente afeta o objetivo/resultado;
- considerar as principais fontes de riscos: infraestrutura, pessoal, processos e tecnologia.

■ 5.3 ANÁLISE DOS RISCOS



A análise do risco se refere ao desenvolvimento da **compreensão sobre o risco** e à **determinação do nível do risco**.

A análise dos riscos deve seguir os seguintes passos:

- avaliar o impacto do risco sobre o objetivo/resultado – o impacto mede o potencial comprometimento do objetivo/resultado (p.ex.: um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto);
- avaliar a probabilidade de ocorrência do risco (p.ex.: um evento cuja ocorrência seja quase certa de acontecer é um evento de alta probabilidade);
- definir o nível do risco com base na matriz **probabilidade x impacto**.

A matriz define o nível de riscos a partir da combinação das escalas de probabilidade e de impacto.

A probabilidade é a chance de o evento ocorrer dentro do prazo previsto para se alcançar o objetivo/resultado. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final.

As escalas podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade e impacto.

Geralmente, utilizam-se escalas qualitativas de probabilidade e de impacto com amplitude de até cinco níveis:

Escala de probabilidade (1 a 5):

- 1_ **raro:** acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
- 2_ **pouco provável:** o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo.
- 3_ **provável:** repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.
- 4_ **muito provável:** repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerá nesse horizonte.
- 5_ **praticamente certo:** ocorrência quase garantida no prazo associado ao objetivo.

Escalas de impacto (1 a 5):

- 1_ **muito baixo:** compromete minimamente o atingimento do objetivo; para fins práticos, não altera o alcance do objetivo/resultados.
- 2_ **baixo:** compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultados.
- 3_ **médio:** compromete razoavelmente o alcance do objetivo/resultados.
- 4_ **alto:** compromete a maior parte do atingimento do objetivo/resultados.
- 5_ **muito alto:** compromete totalmente ou quase totalmente o atingimento do objetivo/resultados.

Um exemplo de análise de risco

Ex.: O TCU tem como meta a instrução de um certo número de processos em um mês. Foram identificados os seguintes eventos de risco que poderiam afetar o cumprimento dessa meta: a) absenteísmo de servidores acima do esperado; e b) perda da base de dados do e-TCU, sem possibilidade de recuperação.

Análise do risco (a): absenteísmo

- Impacto: alto
- Probabilidade: pouco provável

Análise do risco (b): perda da base de dados

- Impacto: muito alto
- Probabilidade: rara

Para definir o nível dos riscos, utiliza-se a matriz abaixo.

Impacto	Muito Alto	15 Risco (b)	19	22	24	25
	Alto	10	14 Risco (a)	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito baixo	1	2	4	7	11
		Raro	Pouco provável	Provável	Muito provável	Praticamente certo
		Probabilidade				

Nível do risco (a): 14 | Nível do risco (b): 15

Figura 2: matriz Impacto x Probabilidade (fonte Seplan)

Não existe uma escala padrão absoluta para matrizes de avaliação de nível de risco. O gestor deve considerar o nível de análise que vai agregar valor à sua tomada de decisão e que não implica esforço analítico desnecessário. A título ilustrativo, apresentamos mais duas matrizes.

Matriz Simples de Avaliação e Resposta a Riscos

IMPACTO ↑	Alto impacto e baixa probabilidade Resposta: Elaborar plano de contingência	Alto impacto e alta probabilidade Resposta: Adotar procedimentos de controle
	Baixo impacto e baixa probabilidade Resposta: Tolerar	Baixo impacto e alta probabilidade Resposta: Adotar procedimentos de controle
	PROBABILIDADE →	

Figura 3: Matriz 2 x 2 de resposta a risco (INTOSAI GOV 9130, traduzido e adaptado)

Modelo de Gerenciamento de Risco

		AÇÕES DE GERENCIAMENTO DE RISCO		
IMPACTO ↑	Alto	6 Considerável esforço de gerenciamento é necessário	8 Indispensável gerenciar e monitorar riscos	9 Indispensável extensivo gerenciamento de risco
	Médio	3 Riscos podem ser aceitos, com monitoramento	5 Esforço de gerenciamento é necessário	7 Esforço de gerenciamento exigido
	Baixo	1 Aceitar Riscos	2 Aceitar, mas monitorar riscos	4 Gerenciar e monitorar riscos
		Baixa	Média	Alta
		PROBABILIDADE		

Figura 4: Matriz 3 x 3 de gerenciamento de risco (Secretaria do Tesouro do Canadá)

5.4 AVALIAÇÃO DOS RISCOS



A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável.

O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Espera-se que, com os resultados do tratamento, o nível de risco residual fique abaixo do limite de exposição.

Matriz Simples de Risco e Tolerância ao Risco

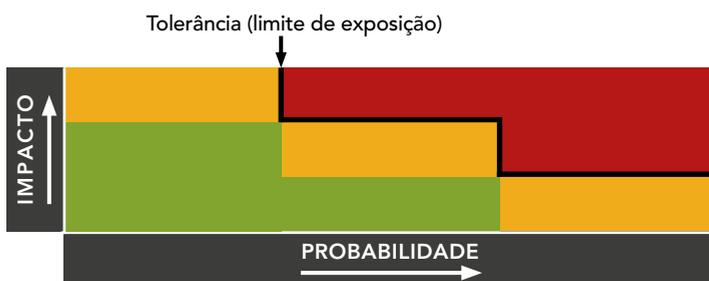


Figura 5: Matriz de avaliação dos riscos (UK Orange Book 2004 – traduzido e adaptado)

A avaliação dos riscos deve seguir os seguintes passos:

- identificar, na matriz probabilidade x impacto, os riscos cujos níveis estão acima do limite de exposição a risco (faixa vermelha da matriz);
- identificar, para os riscos acima do limite, as respectivas fontes, causas e eventuais consequências sobre a organização como um todo;
- identificar os riscos que estão abaixo do limite de exposição:

para os riscos cujos níveis se encontram na faixa amarela, deverá ser avaliada a necessidade de monitoramento;

os riscos cujos níveis se encontram na faixa verde, poderão ser aceitos, sem que qualquer providência tenha que ser tomada.

LIMITES DE EXPOSIÇÃO AO RISCO

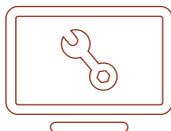
Riscos acima do limite de exposição: **faixa vermelha**

Riscos com necessidade de monitoramento: **faixa amarela**

Riscos que podem ser aceitos: **faixa verde**

A avaliação dos riscos fornece subsídios para a tomada de decisão, não se constituindo em fator determinante para eventual tratamento do risco. Ou seja, cabe ao gestor, diante da lista de riscos ordenados por nível de risco, decidir quais merecerão ações mitigadoras.

5.5 TRATAMENTO DOS RISCOS



Compreende o planejamento e a realização de ações para **modificar o nível do risco**.

O nível do risco pode ser modificado por meio de **medidas de resposta ao risco** que mitiguem, transfiram ou evitem esses riscos.

O tratamento dos riscos deve seguir os seguintes passos:

- identificar medidas de resposta ao risco;
- avaliar a viabilidade da implantação dessas medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais do tratamento etc.);
- decidir quais serão implementadas;
- elaborar plano de implementação das medidas para inclusão nos planos institucionais.

A identificação das medidas de resposta ao risco, assim como a identificação de riscos, deve ser realizada em oficinas de trabalho ou, conforme o caso, pelo próprio gestor do risco, com a participação de pessoas que conheçam bem o objeto de gestão de riscos.

Devem ser utilizadas técnicas/ferramentas que permitam a identificação da maior quantidade de medidas de resposta ao risco, tais como *brainstorming*, *brainwriting*, entrevistas, visitas técnicas, pesquisas etc.

São dicas que facilitam a identificação de medidas de resposta ao risco:

- responder às seguintes perguntas-chave:
 - que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco?
 - que medidas poderiam ser adotadas para reduzir o impacto do risco no objetivo/resultado?
 - é possível adotar medidas para transferir o risco?
- considerar as fontes e causas dos riscos – a princípio, as medidas devem atacar as causas do risco, de modo a reduzir a probabilidade de ocorrência, ou também podem consistir em planos de contingência que amenizem os impactos, caso o risco se concretize, ou uma combinação das duas abordagens;
- na decisão quanto à implantação das medidas de resposta ao risco, considerar a quantidade e o nível dos riscos mitigados por cada medida, bem como o grau de redução do nível do risco gerado pela medida.

As medidas mitigadoras podem envolver, por exemplo, a adoção de controles, o redesenho de processos, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de TI, a adequação da estrutura organizacional, entre outros.

Para permitir uma gestão mais efetiva dos riscos, é importante o registro das informações, conforme ilustrado abaixo.

Tabela de Gestão de Riscos

Objeto da gestão de riscos*:

OBJETIVO	RISCO	NÍVEL DO RISCO	CAUSA	CONSEQUÊNCIA	TRATAMENTO

* projeto, atividade, etc.

Exemplo Simplificado (meramente ilustrativo)

Macroprocesso: Auxílio ao Congresso Nacional

Processo: Participação em audiência pública no CN

OBJETIVO	RISCO	NÍVEL DO RISCO	CAUSA	TRATAMENTO
Apresentar posicionamento do TCU sobre o assunto em discussão	Comunicar posicionamento não condizente com o do TCU	14	Conteúdo da apresentação pode levar a interpretações diversas da intenção do apresentador	<ul style="list-style-type: none"> Alertar palestrante quanto à revisão sob essa ótica Submeter a revisão de outro servidor qualificado com antecedência
	Ser questionado sobre assunto diverso ao do objeto da audiência pública	23	Existência de questões com grande repercussão na mídia por ocasião da audiência	<ul style="list-style-type: none"> Passar orientação clara para o palestrante Preparar-se previamente Simular possíveis perguntas Padronizar respostas

Obs: neste caso, não foi preenchida a coluna de consequências, o que, dependendo do contexto, é perfeitamente legítimo.

■ 5.6 MONITORAMENTO



Compreende o **acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos**, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

O monitoramento tem três dimensões:

- o funcionamento do Sistema de Gestão de Riscos do TCU;
- a implementação e os resultados do tratamento de riscos;
- a evolução do nível dos riscos que não mereceram tratamento por parte do gestor.

O monitoramento do funcionamento do Sistema de Gestão de Riscos está a cargo da Secretaria de Planejamento, Governança e Gestão (Seplan), dos coordenadores setoriais e da alta administração do TCU.

O monitoramento das ações de tratamento de riscos envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras.

O monitoramento deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

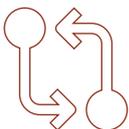
O monitoramento é parte integrante do processo de gestão e de tomada de decisão e deve acompanhar o ciclo de planejamento institucional. O monitoramento deve ser efetivo sem onerar demasiadamente o processo.

Os riscos-chave identificados serão monitorados a cada ciclo de avaliação da estratégia organizacional pela Seplan, em conjunto com o gestor do risco.

O monitoramento consistirá na atualização da análise e avaliação do risco, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas.

O monitoramento dos riscos de processos, unidades e projetos será realizado pelo respectivo gestor do risco.

■ 5.7 COMUNICAÇÃO



Refere-se à **identificação das partes interessadas** e ao **compartilhamento de informações** relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo.

Comunicar riscos é fornecer as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente.

Podemos dividir esse fluxo de comunicação em duas direções: **vertical** e **horizontal**.

A **comunicação vertical** pode ser no sentido da base para a cúpula ou vice-versa, proporcionando que a cúpula da organização seja informada de riscos por todas as unidades organizacionais e que os servidores tenham ciência dos principais riscos que afetam a organização.

Por sua vez, a **comunicação horizontal** é importante para que os riscos de um processo que envolva diferentes unidades, às vezes, de diferentes secretarias-gerais, sejam conhecidos igualmente por todos os que trabalham nesse processo.

■ 5.8 MELHORIA CONTÍNUA



Compreende o aperfeiçoamento ou ajuste de aspectos da gestão de riscos avaliados no monitoramento.

A melhoria contínua pode ser entendida em duas dimensões: uma relativa ao próprio Sistema de Gestão de Riscos do TCU, a cargo da Comissão de Coordenação-Geral (CCG); e outra relacionada aos resultados do monitoramento sobre a efetividade do tratamento do risco, a cargo dos gestores de risco.

6. SISTEMA DE GESTÃO DE RISCOS DO TCU (SGR/TCU)

O Sistema de Gestão de Riscos do Tribunal de Contas da União consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos através de toda a organização e compreende, entre outros: política de gestão de riscos, estruturas organizacionais, planos, relacionamentos, responsabilidades, atividades, processos e recursos.

■ 6.1 INSTÂNCIAS E RESPONSABILIDADES



De acordo com a Política de Gestão de Riscos do TCU, são instâncias responsáveis pelo Sistema de Gestão de Riscos:

- Plenário
- Presidente
- Comissão de Coordenação-Geral (CCG)
- Secretaria de Planejamento, Governança e Gestão (Seplan),
- Unidades básicas
- Coordenadores setoriais de gestão de riscos
- Gestores de riscos
- Secretaria de Auditoria Interna (Seaud)

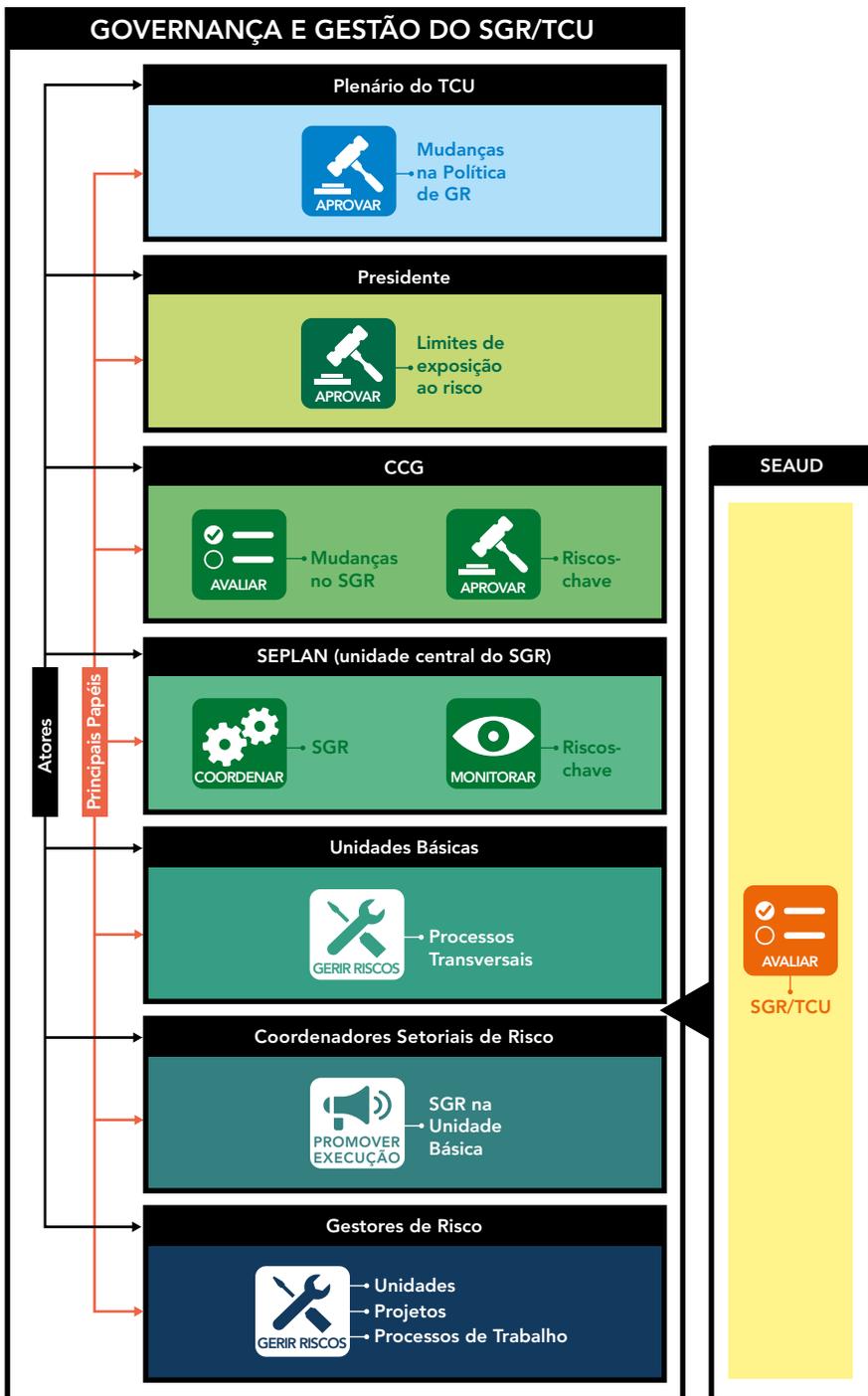


Figura 6: Governança e Gestão do SGR/TCU (Seplan)

A **Seplan** desempenha o papel de unidade central de coordenação e supervisão da gestão de riscos no TCU.

Coordenador setorial de gestão de riscos é a pessoa ou unidade responsável por:

- coordenar ações e promover a execução do SGR/TCU no âmbito da unidade básica a que se vincula;
- prover informações à unidade central do SGR/TCU;
- apoiar os dirigentes e gestores de riscos no desempenho das suas competências.

Gestor de risco é a pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco.

Os gestores de riscos têm a atribuição de executar as atividades do processo de gestão de riscos dos objetos de gestão sob sua responsabilidade.

Os gestores de risco podem ser:

- responsáveis por um processo, atividade ou ação de plano institucional;
- gestores de projetos;
- especialistas seniores;
- gestores de nível operacional;
- dirigentes de unidade básica, de coordenação-geral, de unidade e chefes de gabinete.

Os coordenadores-gerais, dirigentes de unidades básicas e de unidade são gestores de risco de objetos de gestão que tenham natureza transversal no âmbito das unidades sob sua responsabilidade.

Os gestores de risco devem:

- identificar os objetos de gestão sob sua responsabilidade (projetos, processos, atividades, ações etc.);
- conduzir o respectivo processo de gestão de riscos, conforme descrito no item 5;
- comunicar aos respectivos coordenadores setoriais e à Seplan os resultados das avaliações de risco realizadas nos objetos de gestão sob sua responsabilidade.

A **Seplan**, como unidade central do SGR/TCU, é responsável por:

- identificar, entre os riscos comunicados pelos gestores de risco e aqueles identificados diretamente pela Seplan, os riscos que, em função do impacto potencial no Tribunal, devem ser conhecidos pela alta administração (**riscos-chave**);
- identificar e avaliar os riscos nas unidades que não estão sob a responsabilidade de um coordenador setorial e aqueles referentes ao mandato e aos objetivos estratégicos do TCU;
- monitorar os riscos-chave.

Os possíveis riscos-chave identificados e consolidados pela Seplan deverão ser levados à **CCG** para validação. Os riscos-chave validados serão objeto de monitoramento por parte da Seplan e suas situações deverão ser comunicadas periodicamente à alta administração (Presidente e CCG). Compete ao **Presidente do TCU**, com base em proposta elaborada pela Seplan e encaminhada pela CCG, definir os limites de exposição a riscos de abrangência institucional. Os riscos-chave serão avaliados em confronto com esse limite. Por fim, cabe ao **Plenário** avaliar propostas de mudanças na política de gestão de riscos.

Os dirigentes de unidades deverão monitorar os riscos de todos os objetos de gestão sob sua responsabilidade.

Quando houver dúvida sobre a identificação do gestor de determinado risco no âmbito interno das unidades ou entre unidades da mesma unidade básica, cabe ao superior imediato decidir.

Na hipótese de dúvida quanto à responsabilidade pela gestão de determinado risco entre unidades de unidades básicas distintas, cabe à CCG decidir.

A **Seaud** deverá avaliar o SGR/TCU, especialmente quanto à adequação e suficiência dos mecanismos de gestão de riscos estabelecidos, da eficácia da gestão de riscos-chave e da conformidade das atividades executadas com a política de gestão de riscos.

■ 6.2 FUNCIONAMENTO DO SISTEMA DE GESTÃO DE RISCOS



O funcionamento do SGR dependerá da natureza e da abrangência do objeto da gestão de riscos.

COMPETÊNCIAS CONSTITUCIONAIS, OBJETIVOS ESTRATÉGICOS E MACROPROCESSOS

A Seplan é a unidade responsável por gerenciar os riscos relativos às competências constitucionais, aos objetivos estratégicos e aos macroprocessos do TCU.

Para executar o SGR/TCU no âmbito desses objetos, a Seplan deverá:

- identificar os riscos e as respectivas medidas mitigadoras com os ministros, os procuradores, os chefes de gabinete, a CCG e os dirigentes;
- definir critérios para identificação de riscos-chave;
- monitorar os riscos-chave;
- avaliar a pertinência de incluir medidas mitigadoras vinculadas aos riscos-chave nos planos institucionais.

PROCESSOS

A gestão de riscos dos processos não depende do seu mapeamento. A realização de oficinas com servidores que conhecem o processo em profundidade geralmente é suficiente para identificar os principais riscos e as respectivas medidas mitigadoras.

A Seplan definirá critérios para priorização dos processos que deverão ser objeto de gestão de riscos, considerando a transversalidade e o impacto desses processos nos objetivos estratégicos do Tribunal. Essa priorização não exclui a possibilidade de os gestores de risco decidirem gerir riscos de processos de trabalho sob sua responsabilidade.

A partir dos processos priorizados, a Seplan e os responsáveis pelo processo definirão a equipe que irá participar do processo de identificação dos riscos e das medidas mitigadoras (quantidade, perfil, lotação etc.).

A gestão dos riscos em processos de trabalho deverá seguir os passos descritos na seção 5, com o apoio da tabela específica contida no Anexo.

Possíveis riscos-chave, identificados a partir de critérios definidos previamente pela Seplan, deverão ser informados ao dirigente da unidade ou da unidade básica, conforme o caso, e à Seplan.

Os riscos-chave deverão ser monitorados pela Seplan e acompanhados pela CCG.

UNIDADES

O dirigente deverá gerenciar os riscos da unidade sob sua responsabilidade, considerando as seguintes dimensões:

- riscos como subsídio para tomada de decisão quanto à inclusão ou não de ações em planos institucionais;
- riscos referentes a ações e metas previstas nos respectivos planos institucionais;
- riscos relacionados às entregas que cabem à unidade, conforme previsto no rol de suas atribuições e competências;

- riscos que comprometam o funcionamento da unidade.

Sob a ótica do processo de planejamento, na definição de estratégias e ações, deverão ser considerados os riscos como parte do processo decisório para sua inclusão ou não no plano.

Depois de definidas as ações que farão parte do plano da unidade, as respectivas medidas mitigadoras para esses riscos também farão parte do plano.

A identificação dos riscos da unidade, das estratégias e das ações será realizada de acordo com a metodologia de planejamento do Tribunal.

Se o dirigente da unidade identificar algum risco que possa ser caracterizado como risco-chave para o TCU, a partir de critérios pré-definidos pela Seplan, deverá informar à Seplan e ao titular da respectiva unidade básica.

PROJETOS

Todos os gestores de projetos realizarão a gestão dos riscos a eles associados, conforme o processo descrito na seção 5. Segundo o *Project Management Body of Knowledge* (PMBOK) de 2004, "Projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo." Enquadram-se nessa definição, por exemplo, os trabalhos de Especialista Sênior aprovados pela CCG e os projetos de TI.

Se o gestor do projeto identificar algum risco que possa ser caracterizado como risco-chave para o TCU, deverá informar à Seplan e ao titular da unidade técnica responsável pelo projeto.

■ 6.3 INTEGRAÇÃO DA GESTÃO DE RISCOS COM O PLANEJAMENTO ESTRATÉGICO



Os riscos constituem insumo para o diagnóstico institucional do processo de planejamento estratégico.

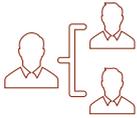
Ao se formular a estratégia institucional, deverão ser considerados os riscos intrínsecos àquela estratégia (COSO 2017). Deve ser considerado, também, o risco de a estratégia não estar alinhada à missão, à visão e às competências constitucionais do TCU.

Depois de estabelecida a estratégia, as medidas mitigadoras constituirão ações constantes dos planos operacionais.



Figura 7: Avaliação de Riscos Estratégicos e Alinhamento de Objetivos (Coso 2017 - traduzido para o Português)

■ 6.4 ATUAÇÃO DOS COORDENADORES SETORIAIS DE RISCO (CSR)



Espera-se que o coordenador setorial de risco atue como incentivador da gestão de riscos na sua unidade básica com os seus gestores. Essa atuação pode incluir a sugestão de processos de trabalho que devam ter seus riscos geridos, bem como o acompanhamento da evolução da gestão de riscos nas unidades e das medidas mitigadoras a cargo dos responsáveis por implementá-las.

Os coordenadores exercerão o papel de interlocução entre a Seplan e os gestores de risco das unidades sob sua responsabilidade.



REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. NBR ISO 31000: **Gestão de Riscos: Princípios e Diretrizes**. Rio de Janeiro, 2009.

BRASIL. Tribunal de Contas da União. Resolução-TCU nº 1.148, de 2 de março de 1984. **Dispõe sobre a política de gestão de riscos do Tribunal de Contas da União**. Disponível em: <<http://portal.tcu.gov.br/biblioteca-digital/politica-de-gestao-de-riscos-do-tcu.htm>>. Acesso em: março, 2018.

_____. _____. Portaria-Segecex nº 9, de 18 de maio de 2017. **Roteiro de Auditoria de Gestão de Riscos**. Disponível em: <<http://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm>>. Acesso em: março, 2018.

CANADÁ. Secretaria do Conselho do Tesouro do Canadá. **Framework for the management of risk**. Ottawa, 2010a. Disponível em: <<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422§ion=text>>. Acesso em: março, 2018.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. **Enterprise Risk Management - Integrating with Strategy and Performance**. COSO 2017. Disponível em: <<https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>>. Acesso em: março de 2018

INTOSAI (International Organization of Supreme Audit Institutions). Subcomitê de Normas de Controle Interno. **Diretrizes para Normas de Controle Interno do Setor Público – Informações Adicionais sobre Gestão de Risco nas Entidades**. INTOSAI GOV 9130. Viena, 2007. Tradução: Antonio Alves de Carvalho Neto. Brasília, 2013

REINO UNIDO (UK). HM Treasury. **Management of Risk - Principles and Concepts - The Orange Book**. HM Treasury do HM Government, 2004. PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge: PMBOK Guide**, 3a. edição, 2004, PMI.

GLOSSÁRIO

Coordenador setorial de gestão de riscos: pessoa ou unidade responsável por coordenar ações e promover a execução do SGR/TCU no âmbito da unidade básica a que se vincula, prover informações à unidade central, bem como apoiar os dirigentes e os gestores de riscos no desempenho das competências.

Evento: um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

Gestão de riscos: atividades coordenadas para dirigir e controlar a organização no que se refere a riscos e oportunidades.

Gestor de risco: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco.

Nível do risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e seu impacto nos objetivos.

Objeto de gestão de riscos (objeto de gestão): qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos do TCU.

Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos.

Risco: possibilidade de que um evento afete negativamente o alcance de objetivos.

Risco-chave: risco que, em função do impacto potencial ao TCU, deve ser conhecido pela alta administração.

Sistema de Gestão de Riscos do Tribunal de Contas da União (SGR/TCU): consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, a implementação, o monitoramento e a melhoria contínua da gestão de riscos na organização e compreende, entre outros: política, estruturas organizacionais, planos, relacionamentos, responsabilidades, atividades, processos e recursos.

ANEXO

Tabela de Análise e Avaliação de Risco – Processos de Trabalho

Processo: (identificar o processo de trabalho)

ÁREA ou AGENTE	ETAPA / ATIVIDADE (Sequência e descrição)	OBJETIVO DA ETAPA/ ATIVIDADE	DESCRIÇÃO DOS RISCOS (Eventos de risco)	CONTROLES EXISTENTES		NÍVEL DO RISCO (Residual - após controle)	AVALIAÇÃO DA EXPOSIÇÃO AO RISCO (Se abaixo ou acima do limite de exposição) <i>A (aceitável)</i> <i>NA (não aceitável)</i>
				DES- CRI- ÇÃO	RES- PON- SÁVEL		



Responsabilidade pelo Conteúdo

Secretaria de Planejamento,
Governança e Gestão (Seplan)

Projeto gráfico, diagramação e capa

Secretaria de Planejamento,
Governança e Gestão (Seplan)

Secretaria de Comunicação (Secom)

Núcleo de Criação e Editoração (NCE)

Endereço

TRIBUNAL DE CONTAS DA UNIÃO

Secretaria de Planejamento,
Governança e Gestão (Seplan)

SAFS Quadra 4 Lote 1

Edifício Anexo II Sala 441

70.042-900 Brasília - DF

(61) 3316 7374

seplan@tcu.gov.br

Ouvidoria

0800 644 1500

ouvidoria@tcu.gov.br

Impresso pela Sesap/Segedam



Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.

www.tcu.gov.br