Metodologia de Gestão de Riscos e Continuidade do Negócio

TCETO

Tribunal de Contas do Estado do Tocantins

Presidente
Conselheiro Alberto Sevilha

Vice-presidente
Conselheira Doris de Miranda Coutinho

Corregedor
Conselheiro José Wagner Praxedes

Ouvidor
Conselheiro Manoel Pires dos Santos

Diretor do Instituto de Contas 5 de Outubro
Conselheiro André Luiz de Matos Gonçalves

Presidente da 1° Câmara
Conselheiro Napoleão de Souza Luz Sobrinho

Presidente da 2° Câmara
Conselheiro Severiano José Costandrade de Aguiar

Conselheiros Substitutos
Adauton Linhares da Silva
Fernando César Benevenuto Malafaia
Leondiniz Gomes
Márcio Aluízio Moreira Gomes
Moisés Vieira Labre

Ministério Público de Contas
Procurador-Geral
Oziel Pereira dos Santos

Procuradores
José Roberto Torres Gomes
Marcos Antonio da Silva Modes
Zailon Miranda Labre Rodrigues

Tribunal de Contas do Estado do Tocantins
Av. Teotônio Segurado, Quadra 102 Norte Conjunto 01, Lotes 01 e 02.
77006-002 – Palmas – TO
Fone: (63) 3232-5800
www.tceto.tc.br

Elaboração

Assessoria Especial de Planejamento e Desenvolvimento Organizacional

Heverson de Almeida Braga

Comitê Gestor de Riscos

Dimas Baía de Castro Filho

Heverson de Almeida Braga

Dênia Maria Almeida da Luz Soares

André Luiz Lobo Rocha

Arlan Marcos Lima Sousa

David Siffert Torres

Francisco de Assis dos Santos Júnior

Carlos Neri de Souza

Aida Maria do Amaral

Marcus Vinicius Schmitz

Dhenia Gerhardt

Revisão Ortográfica

Rafaela Martins Melo Medeiros

Projeto Gráfico/Diagramação

João Kennedy Batista Lima

Heverson de Almeida Braga

Ronaldo Cordeiro de Toledo Gomes

Dados Internacionais de Catalogação na Publicação (CIP)

Biblioteca Conselheiro José Ribamar Meneses (TCETO

T631m **Tocantins. Tribunal de Contas. Assessoria Especial de Planejamento e Desenvolvimento Organizacional**

Metodologia de gestão de riscos e continuidade do negócio. [recurso eletrônico] / Tribunal de Contas do Estado do Tocantins. Assessoria Especial de Planejamento e Desenvolvimento Organizacional. --- Palmas, TO: TCE-TO, 2025.

E-Book:PDF(44 p.):il. color.

Disponível em : https://www.tceto.tc.br/governanca-e-gestao/metodologia-de-gestao-de-risco/

1.Gerenciamento de riscos - Metodologia. 2. Tribunal de Contas. 3. Negócios. 4. Gestão organizacional

1. Título.

CDD - 352.37

CDU - 35:658.5

Catalogação na publicação: SMS-CRB-2/635

Mensagem do Presidente

É com grande satisfação que apresento a Metodologia de Gestão de Riscos do Tribunal de Contas, instrumento concebido para fortalecer a capacidade institucional desta Corte no enfrentamento dos desafios contemporâneos da administração pública. Em um cenário cada vez mais complexo e dinâmico, a adoção de práticas eficazes de governança e controle interno torna-se imprescindível para a promoção da integridade, da eficiência e da *accountability* nas ações desenvolvidas por este Tribunal.

A gestão de riscos não é apenas uma exigência normativa ou uma tendência administrativa, trata-se de uma abordagem estratégica essencial para o aprimoramento contínuo da atuação institucional. Ao identificar, avaliar, tratar e monitorar os riscos que possam comprometer o alcance de nossos objetivos, estamos exercendo, de forma proativa, a responsabilidade que nos foi conferida pela sociedade: zelar pela boa governança e pelo uso adequado dos recursos públicos.

A construção desta metodologia representa um marco importante em nossa trajetória rumo à excelência em gestão. Trata-se de um modelo pensado de forma realista, objetiva e alinhada às melhores práticas nacionais e internacionais. Seu desenvolvimento contou com a valiosa contribuição de servidores comprometidos com a inovação, a responsabilidade e a busca constante por melhores resultados. Esta iniciativa consolida, ainda, os avanços já conquistados em nosso processo de modernização institucional.

É importante ressaltar que a gestão de riscos deve ser compreendida como um processo contínuo e integrado ao cotidiano do Tribunal. Não se trata de um documento estático, mas de uma ferramenta viva, que exige participação ativa, visão sistêmica e colaboração de todos os setores e níveis hierárquicos. Todos os membros, servidores e unidades desempenham papel essencial nesse processo, contribuindo com sua expertise e comprometimento para a construção de uma cultura organizacional voltada à prevenção e à resiliência.

A adoção dessa metodologia reforça o compromisso desta Presidência com uma administração pública responsável, transparente e orientada a resultados. Mais do que um avanço técnico, trata-se de um salto de maturidade institucional. Cada membro, servidor e unidade desempenha papel essencial nesse processo, contribuindo com sua expertise e comprometimento para consolidar uma cultura organizacional orientada à prevenção e à resiliência.

Convido, portanto, cada integrante desta Corte a abraçar este desafio com entusiasmo e senso de pertencimento. A jornada rumo à excelência em governança é coletiva e contínua.

Cons. Alberto Sevilha
Presidente TCETO

Sumário

1 Introdução

A governança pública pode ser conceituada como o conjunto de mecanismos, processos, normas e práticas que orientam, coordenam e controlam a atuação do Estado na formulação, implementação e avaliação de políticas públicas, promovendo a participação democrática, a transparência, a prestação de contas e a efetividade na gestão dos recursos e serviços públicos. Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a governança pública envolve a capacidade dos governos de atuar com integridade, competência e abertura, buscando o bem comum por meio de instituições inclusivas, resilientes e responsáveis. Desse modo, transcende a mera administração burocrática ao integrar múltiplos atores públicos, privados e da sociedade civil em processos decisórios colaborativos, voltados à promoção do desenvolvimento sustentável e ao fortalecimento da confiança na esfera pública.

Nesse contexto, a governança de riscos configura-se como um componente essencial da governança pública, mediante a estruturação de mecanismos capazes de identificar, avaliar, tratar e monitorar incertezas que possam comprometer o alcance dos objetivos institucionais e a qualidade dos serviços prestados à população. Sua implementação efetiva confere maior robustez aos processos decisórios, permitindo que os gestores públicos atuem de forma proativa diante de potenciais ameaças e oportunidades, assegurando maior resiliência organizacional.

Desta forma, a governança de risco promove uma cultura institucional fundamentada na prevenção, na responsabilidade e na melhoria contínua, reforçando o compromisso do Estado com a entrega de resultados à sociedade e com a sustentabilidade das políticas públicas a longo prazo.

O processo de gerenciamento de riscos, por sua vez, visa assegurar a continuidade, a eficiência e a transparência das atividades de uma instituição pública, sobretudo em um cenário marcado por constantes mudanças e elevada complexidade. No âmbito das instituições públicas, os riscos podem assumir diversas formas, abrangendo desde riscos financeiros, operacionais e de conformidade até aqueles relacionados à reputação e à segurança da informação, entre outros. A gestão eficaz desses riscos é crucial não apenas para a proteção dos recursos públicos, mas também para a confiança da sociedade nas ações governamentais.

Essa metodologia segue diretrizes de boas práticas internacionais, devidamente adaptadas à realidade do setor público, considerando as particularidades legais, regulamentares e éticas que regem a administração pública. Com isso, visa garantir que os riscos sejam geridos de maneira eficiente, transparente, em conformidade com os princípios da governança pública, proporcionando um ambiente institucional mais seguro e resiliente, capaz de responder de forma ágil e eficaz às diversas situações.

2 Histórico

Em 2004, a Organização Internacional das Instituições Superiores de Controle (INTOSAI) publicou a norma **INTOSAI GOV 9130**, com o propósito de fornecer diretrizes complementares aos padrões de controle interno no setor público, com ênfase específica na gestão de riscos organizacionais. Intitulada Diretrizes para *Normas de Controle Interno do Setor Público - Informações Adicionais sobre Gestão de Riscos às entidades*, a publicação visa apoiar os órgãos públicos no desenvolvimento e na implementação de estruturas eficazes de gerenciamento de riscos, alinhadas ao modelo de referência **COSO ERM**, adaptado às particularidades do setor público.

Posteriormente, em 2014, a Associação dos Membros dos Tribunais de Contas do Brasil (ATRICON) editou a **Resolução nº 4/2014**, que estabelece diretrizes relacionadas à criação, organização, funcionamento e avaliação dos sistemas de controle interno e de gestão de riscos no âmbito dos próprios Tribunais de Contas. O principal objetivo da referida resolução foi fortalecer e aprimorar os sistemas de controle interno das Cortes de Contas, promovendo maior eficiência, transparência e conformidade com as boas práticas de governança pública.

No âmbito do Tribunal de Contas do Estado do Tocantins (TCETO), esse movimento institucional em prol da governança e do gerenciamento de riscos foi formalizado, em 2019, por meio da **Resolução Administrativa do Tribunal Pleno nº 6/2019**, que aprovou a política de governança organizacional e compliance. Entre os instrumentos instituídos por essa norma, destaca-se a implementação de um sistema de gestão de riscos, com o objetivo de identificar, avaliar e tratar os riscos críticos à organização, fortalecendo a governança interna e promovendo maior eficácia dos processos, bem como transparência nas atividades desenvolvidas pelo Tribunal.

Dando continuidade a essa agenda estratégica, em 2024, o TCETO instituiu, por meio da **Portaria nº 199/2024**, a comissão para a implantação da gestão de riscos nos processos administrativos. A referida comissão foi incumbida de promover a integração dos conceitos e práticas de gerenciamento de riscos aos procedimentos internos do Tribunal, com vistas a fortalecer a eficácia e a segurança das operações administrativas, além de assegurar a conformidade com as normas e regulamentos vigentes.

3 Governança e gestão de riscos do TCETO

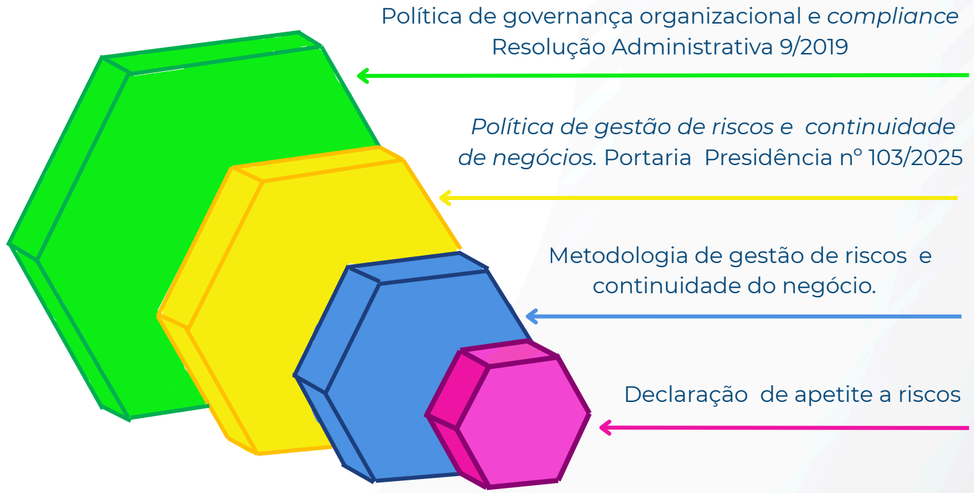
ico

No ano seguinte, em 2025, por meio da Portaria nº 103/2025, o Tribunal implantou a política de gestão de riscos e continuidade do negócio, estabelecendo princípios, diretrizes, competências e responsabilidades a serem observados em todos os níveis institucionais — estratégico, tático e operacional. Essa iniciativa visa consolidar uma abordagem integrada e eficaz de gestão de riscos, assegurando a continuidade das operações do TCETO mesmo diante de situações adversas e garantindo, assim, maior segurança, transparência e eficiência na administração pública.

A consolidação da política de governança organizacional, da política de gestão de riscos e continuidade do negócio, da metodologia de gestão de riscos e da declaração de apetite ao risco representa um marco significativo no fortalecimento da governança institucional do Tribunal de Contas do Estado do Tocantins, conforme ilustrado na Figura 1. A política configura-se como instrumento normativo de caráter estratégico, responsável por estabelecer os princípios, diretrizes, objetivos e responsabilidades que orientam a atuação institucional no que se refere à governança, à gestão de riscos e à continuidade do negócio. A metodologia, por sua vez, constitui o conjunto de processos, critérios e procedimentos operacionais sistematizados que viabilizam a implementação prática da política, permitindo a identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos em consonância com os objetivos institucionais.

Já a declaração de apetite ao risco constitui documento formal que expressa, de forma clara e objetiva, os níveis de risco que a organização está disposta a aceitar em cada uma de suas áreas de atuação, considerando seu perfil estratégico, sua missão institucional e sua capacidade de resposta.

Figura 1: Estrutura do Sistema de gestão de riscos do TCETO.



ico

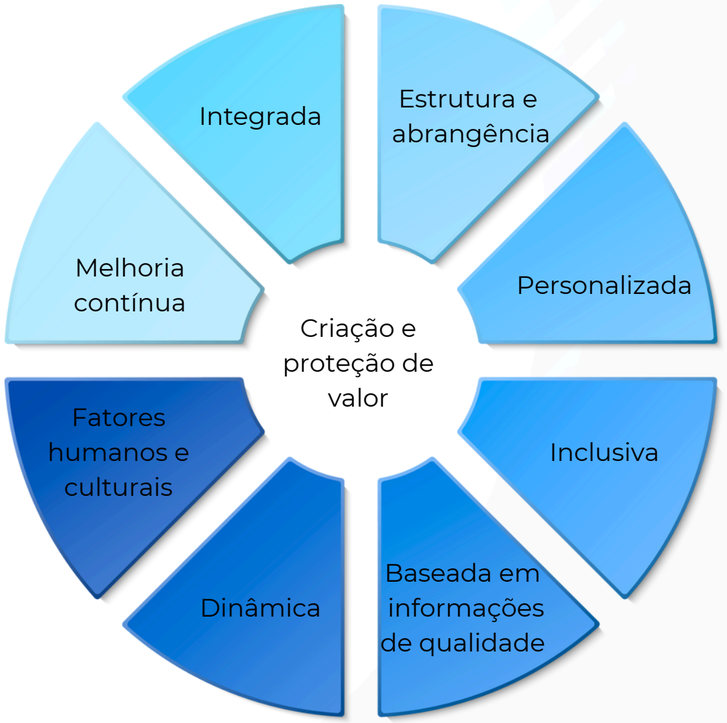
4 Princípios da governança e gestão de riscos

Os princípios de governança e gestão de riscos constituem diretrizes essenciais que orientam a forma como o Tribunal de Contas do Estado do Tocantins estrutura, implementa e sustenta seu sistema de gerenciamento de riscos. Tais princípios expressam o valor, a finalidade e a intenção dessa prática, oferecendo parâmetros que asseguram uma gestão eficaz, eficiente e alinhada às necessidades institucionais. Além disso, servem como referência para o desenvolvimento de políticas, processos e instrumentos que possibilitam à instituição lidar, de maneira sistemática e integrada, com os riscos capazes de comprometer o alcance de seus objetivos organizacionais e estratégicos.

No âmbito do Tribunal de Contas do Estado do Tocantins (TCETO), a observância desses princípios revela-se especialmente relevante, pois favorece a tomada de decisão fundamentada, a transparência na utilização dos recursos públicos e o fortalecimento da confiança da sociedade na atuação da Corte de Contas. Dessa forma, devem ser incorporados à estrutura organizacional e aos processos de governança, assegurando que a instituição esteja preparada para identificar, avaliar, tratar e monitorar os riscos decorrentes das incertezas internas e externas que afetam sua missão.

Assim, conforme ilustrado na Figura 2, os princípios não apenas conferem legitimidade e consistência à gestão de riscos, mas também funcionam como alicerces para a melhoria contínua e para a geração de valor público.

Figura 2: Princípios do sistema de gestão de riscos do TCE-TO.



I. **Integrada**: A gestão de riscos deve ser parte integrante de todos os processos organizacionais, incorporando-se de maneira transversal às atividades estratégicas, táticas e operacionais. Essa integração assegura que a abordagem de riscos esteja permanentemente vinculada ao alcance dos objetivos institucionais.

II. **Estruturada e abrangente**: Uma abordagem estruturada e abrangente favorece resultados consistentes e comparáveis. A governança de riscos deve estar integrada ao sistema de governança e liderança da organização, sendo aplicada em todos os níveis decisórios. As deliberações relacionadas aos riscos devem estar alinhadas à política institucional e ao nível de tolerância previamente definido.

III. **Personalizada**: A estrutura e os processos de gestão de riscos devem ser adaptados ao contexto interno e externo da organização, considerando suas especificidades, os recursos disponíveis e os objetivos institucionais. Essa personalização garante proporcionalidade e maior efetividade no tratamento dos riscos.

IV. **Inclusiva**: O sistema de gestão de riscos deve assegurar o engajamento apropriado e tempestivo das partes interessadas, possibilitando a incorporação de diferentes percepções, experiências e conhecimentos. Essa participação promove maior conscientização, fortalece a legitimidade do processo e assegura uma gestão de riscos mais robusta e fundamentada.

V. **Dinâmica**: Os riscos são dinâmicos e podem emergir, modificar-se ou desaparecer em função de mudanças nos ambientes interno e externo. A gestão de riscos deve antecipar, detectar e responder de forma ágil a tais alterações, promovendo o contínuo aprimoramento dos controles internos e o fortalecimento das ações de prevenção, detecção e correção.

VI. **Baseada em Informações de Qualidade**: As decisões relacionadas à gestão de riscos devem ser fundamentadas em informações históricas, atuais e em projeções futuras, considerando sempre suas limitações e incertezas. Assim, é imprescindível garantir a qualidade, a confiabilidade, a clareza e a disponibilidade das informações às partes interessadas

VII. **Fatores Humanos e Culturais**: A gestão de riscos deve reconhecer que o comportamento humano e a cultura organizacional exercem influência significativa em todos os níveis e etapas do processo. Por essa razão, é necessário promover a conscientização, o engajamento e a capacitação contínua dos membros e servidores, assegurando que o fator humano seja um aliado no fortalecimento da governança

VIII. **Melhoria Contínua:** A gestão de riscos deve ser compreendida como um processo dinâmico e em constante evolução. A aprendizagem organizacional, a revisão periódica de políticas e metodologias e o aprimoramento dos mecanismos de continuidade do negócio são fundamentais para ajustar a governança de riscos às mudanças do ambiente interno e externo.

A melhoria contínua envolve a adoção de práticas sistemáticas de monitoramento, avaliação e retroalimentação, permitindo que a organização identifique falhas, oportunidades de aprimoramento e lacunas em seus processos. Esse movimento permanente fortalece a capacidade institucional de antecipar riscos emergentes e de responder de forma ágil e eficaz às demandas que se apresentam, assegurando maior resiliência organizacional.

Além disso, a melhoria contínua não se limita a ajustes pontuais, mas deve estar vinculada a ciclos de inovação incremental e, quando necessário, a transformações mais profundas. Dessa forma, cria-se um ambiente de aprendizado constante, no qual as experiências acumuladas e os resultados obtidos são utilizados como insumos para aperfeiçoar métodos, ferramentas e práticas de gestão de riscos, alinhando-os às melhores referências nacionais e internacionais.

A cultura organizacional exerce papel determinante na consolidação da melhoria contínua. A instituição deve estimular a participação ativa de todos os servidores, promovendo uma mentalidade voltada à aprendizagem, à inovação responsável e à busca permanente por resultados mais consistentes e sustentáveis. Ao valorizar a contribuição coletiva, o processo de melhoria contínua transforma-se em elemento essencial não apenas da gestão de riscos, mas da própria governança pública.

A gestão de riscos no TCETO fundamenta-se nesses princípios, os quais visam assegurar eficácia, eficiência e transparência nas atividades institucionais, ao mesmo tempo em que estimulam a inovação responsável e a criação de valor público. Essa abordagem considera não apenas os riscos, mas também as oportunidades, aplicando-se de forma universal em todos os níveis organizacionais.

Ademais, busca-se o alinhamento com os objetivos estratégicos da Corte, garantindo que a gestão de riscos contribua, de maneira integrada, para o cumprimento da missão institucional. Ao estimular a inovação responsável, o TCETO promove um ambiente organizacional resiliente, proativo e em constante evolução, alinhado às melhores práticas da administração pública e às exigências legais.

Com ciclos permanentes de revisão e aprimoramento, a gestão de riscos não se apresenta como um processo estático, mas como mecanismo dinâmico e adaptável às mudanças dos contextos interno e externo. A valorização dos fatores humanos e culturais, o fortalecimento dos controles internos e o incentivo à aprendizagem institucional configuram elementos centrais dessa metodologia.

Dessa forma, a gestão de riscos não apenas assegura a continuidade das atividades institucionais, mas também impulsiona o desempenho organizacional e contribui para o fortalecimento da governança pública.

5 Objetivos da governança e gestão de riscos

A gestão de riscos e a continuidade do negócio no Tribunal de Contas do Estado do Tocantins têm como principais objetivos a promoção da eficiência, da transparência e da robustez institucional. Esses objetivos buscam garantir a integridade das operações e a consecução da missão institucional, assegurando o cumprimento dos princípios da governança pública. Assim, os objetivos da gestão de riscos no TCETO incluem:

I. Aumentar a probabilidade de alcance dos objetivos institucionais: maximizar as chances de sucesso na implementação das metas e projetos do Tribunal, por meio de uma gestão de riscos que reduza obstáculos e potencialize oportunidades;

II. Fomentar uma gestão proativa: estimular uma abordagem antecipatória, na qual os riscos sejam identificados e mitigados previamente, garantindo a continuidade das operações e a estabilidade organizacional;

III. Identificar e tratar riscos em toda a organização: promover a identificação e o tratamento de riscos de maneira abrangente, envolvendo todos os processos e atividades do Tribunal, de modo que potenciais riscos sejam geridos de maneira eficaz e integrada;

IV. Melhorar a identificação de oportunidades e ameaças: aperfeiçoar os mecanismos de detecção não apenas de ameaças, mas também de oportunidades, com o objetivo de gerar valor para a instituição e para a sociedade;

V. Fortalecer a governança e gestão institucional: reforçar as práticas de governança, assegurando que a gestão de riscos seja um pilar da administração pública, e que as decisões estejam sempre alinhadas aos princípios de transparência, eficiência e responsabilidade;

VI. Estabelecer uma base confiável para a tomada de decisão: disponibilizar informações e análises precisas, fundamentadas e seguras, que sirvam de base sólida para decisões estratégicas e operacionais;

VII. Assegurar a conformidade legal e normativa dos processos organizacionais: garantir que todos os processos do Tribunal estejam em conformidade com as exigências legais e normativas, mitigando riscos de não conformidade e preservando a integridade institucional;

VIII. Melhorar a prestação de contas à sociedade: Promover a transparência e a *accountability*, aprimorando a comunicação com a sociedade e garantindo que as ações do Tribunal sejam compreendidas, acompanhadas e avaliadas de forma clara e acessível;

IX. Aprimorar o controle interno da gestão: Fortalecer os mecanismos de controle interno, com foco na prevenção, detecção e correção de falhas, de modo a assegurar a boa gestão dos recursos públicos e a eficiência das operações;

X. Aumentar a capacidade da organização de adaptar-se a mudanças: Fortalecer a resiliência organizacional, permitindo que o Tribunal se ajuste de maneira ágil e eficiente a mudanças internas e externas, mantendo sua eficácia mesmo em contextos dinâmicos;

XI. Promover a aprendizagem organizacional: Estimular a contínua evolução e capacitação dos membros e servidores do Tribunal, fomentando uma cultura de aprendizagem organizacional que favoreça a inovação, o aperfeiçoamento contínuo e a adaptação às novas demandas.

Esses objetivos visam garantir que a gestão de riscos no TCETO seja uma ferramenta estratégica e integrada, promovendo a eficiência organizacional, a transparência, a conformidade e a resiliência institucional, ao mesmo tempo em que asseguram o cumprimento da missão institucional e a confiança da sociedade nos serviços prestados. Além disso, busca-se promover e aprimorar a cultura de gestão de riscos na organização, consolidando-a como prática contínua e incorporada à rotina institucional. Esse fortalecimento cultural visa assegurar que a instituição gerencie de maneira adequada os riscos em seus níveis estratégico, tático e operacional, atuando de forma proativa na identificação, avaliação e tratamento dos riscos, de modo a garantir o alcance de seus objetivos e a efetividade de sua missão.

Dessa forma, os objetivos delineados para a gestão de riscos no Tribunal de Contas do Estado do Tocantins consolidam-se como fundamentos estratégicos para o fortalecimento da governança pública. Ao promover uma atuação proativa, transparente e alinhada aos princípios legais e institucionais, a gestão de riscos deixa de ser um mero instrumento de controle, assumindo papel essencial na construção de uma administração mais resiliente, eficiente e orientada à entrega de valor público. Assim, o Tribunal reafirma seu compromisso com a excelência na gestão, com a prestação de contas à sociedade e com a contínua busca pela integridade e pela melhoria dos serviços prestados.

6 Diretrizes da governança e gestão de riscos

A gestão de riscos e a continuidade do negócio constituem elementos essenciais para a boa governança e a sustentabilidade institucional no âmbito do setor público. No contexto do Tribunal de Contas do Estado do Tocantins (TCETO), esses instrumentos assumem papel estratégico, ao contribuírem para a preservação da integridade, da confiabilidade e da eficiência dos processos organizacionais, além de fortalecerem a capacidade de resposta diante de eventos adversos que possam comprometer o cumprimento da missão institucional.

Nesse sentido, as diretrizes apresentadas a seguir orientam a implementação da gestão de riscos e da continuidade do negócio no TCETO, com vistas a garantir sua eficácia, integração e aderência aos padrões mais elevados de governança institucional.

Essas diretrizes, conforme ilustrado na Figura 3, visam garantir que a gestão de riscos e continuidade do negócio no TCETO seja eficaz, integrada e alinhada às melhores práticas de governança, com o objetivo de promover a estabilidade, eficiência e transparência da instituição no cumprimento de sua missão pública.

Figura 3: Diretrizes da governança e gestão de riscos do TCETO

I. Alinhamento com o sistema de governança e gestão

A gestão de riscos deve estar plenamente integrada ao sistema de governança e gestão do Tribunal, de forma a garantir que suas ações estejam em consonância com os objetivos estratégicos da instituição. Busca-se, assim, contribuir para o cumprimento da missão e da visão organizacionais. A gestão de riscos deve apoiar a execução da estratégia institucional, servindo de suporte aos planos estratégico, tático e operacional.

II. Integração à cadeia de valor

A gestão de riscos será implementada de maneira integrada a todos os processos organizacionais e à cadeia de valor do Tribunal, assegurando a identificação, análise e tratamento coordenado dos riscos em todas as áreas e atividades da instituição.

III. Adoção das melhores práticas de governança e gestão de riscos no setor público

O TCETO adotará práticas amplamente reconhecidas de governança institucional, gestão de riscos e continuidade do negócio no âmbito do setor público, assegurando uma abordagem moderna, eficiente e alinhada às normas e recomendações aplicáveis.

IV. Instrumento de apoio à melhoria contínua e à tomada de decisão

A gestão de riscos constituir-se-á em ferramenta estratégica para a promoção da melhoria contínua dos processos organizacionais. Ademais, oferecerá suporte qualificado à tomada de decisão, fornecendo informações claras, objetivas e fundamentadas em análises consistentes.

V. Comunicação clara e objetiva

A comunicação relacionada aos riscos será sempre clara, objetiva e transparente, garantindo a compreensão das partes interessadas quanto às implicações dos riscos identificados e às medidas adotadas. Essa abordagem visa promover o engajamento efetivo e a colaboração de todos os stakeholders envolvidos.

VI. Utilização das melhores informações disponíveis

A gestão de riscos será embasada em dados e informações atualizados, confiáveis e de alta qualidade, assegurando que as decisões sejam fundamentadas nas melhores evidências disponíveis e respaldadas por análises criteriosas.

VII. Fortalecer a transparência e a imagem institucional:

A gestão de riscos será conduzida de maneira transparente, reforçando a credibilidade do Tribunal e fortalecendo sua imagem institucional, assegurando que suas ações sejam compreendidas e confiáveis por todos os públicos, especialmente pela sociedade e pelos órgãos de controle.

7 Instâncias do sistema de gestão de riscos

As Instâncias Responsáveis pelo Sistema de Gestão de Riscos e Continuidade do Negócio no Tribunal de Contas do Estado do Tocantins (TCETO) são:

I. Pleno do Tribunal;

II. Presidente;

III. Comitê Institucional de Governança;

IV. Comitê Gestor de Riscos (CGR);

V. Assessoria Especial de Planejamento e Desenvolvimento Organizacional;

VI. Assessoria de Planejamento;

VII. Assessoria de Desenvolvimento Organizacional;

VIII. Diretoria Geral de Administração e Finanças;

IX. Gestores de Riscos;

X. Instituto de Contas 5 de Outubro;

XI. Núcleo de Controle Interno;

XII. Diretoria Geral de Controle Externo.

I. TRIBUNAL PLENO

Compete ao Pleno do Tribunal acompanhar o sistema de gestão de riscos e continuidade do negócio do TCETO.

II. PRESIDENTE

Compete ao Presidente :

I. Aprovar os critérios e limites de exposição aos riscos;

II. Assegurar os recursos necessários para a implementação eficaz da gestão de riscos e continuidade do negócio.

III. Acompanhar o monitoramento dos riscos institucionais e deliberar quanto às medidas de tratamento propostas pelo Comitê Gestor de Riscos..

III. COMITÊ INSTITUCIONAL DE GOVERNANÇA

I. Propor modificações no sistema de gestão de riscos ;

II. Acompanhar e monitorar o processo de gestão de riscos;

III. Integrar os processos de gestão de riscos na estrutura organizacional do TCETO;

IV. Avaliar a adequação, suficiência e eficácia da estrutura de gestão de riscos;

IV. COMITÊ GESTOR DE RISCOS

Compete ao Comitê Gestor de Riscos:

I. Avaliar propostas de mudanças na política e na metodologia de gestão de riscos e continuidade do negócio do Tribunal de Contas do Estado do Tocantins (TCETO);

II. Acompanhar a situação dos riscos e determinar eventuais ações corretivas, assim como encaminhar o plano consolidado de tratamento de risco a Presidência;

III. Opinar sobre medidas e mudanças de controle a serem implementadas no sistema de gestão de riscos e continuidade do negócio do TCETO.

V. ASSESSORIA ESPECIAL DE PLANEJAMENTO E DESENVOLVIMENTO ORGANIZACIONAL

Compete à Assessoria Especial de Planejamento e Desenvolvimento Organizacional:

I. Coordenar, supervisionar e monitorar o Sistema de Gestão de Riscos do TCETO;

II. Avaliar os planos de tratamento dos riscos propostos pelas unidades;

III. Propor limites de exposição aos riscos.

IV. Informar periodicamente à Alta Administração sobre a situação dos riscos chave;

V. Avaliar e propor mudanças na política e na metodologia de gestão de riscos e continuidade do negócio do TCETO;

Cabe à ASPDO apresentar as informações necessárias para subsidiar a tomada de decisões pelo Comitê de Gestão de Riscos.

VI. ASSESSORIA DE PLANEJAMENTO

Compete à Assessoria de Planejamento:

I. Consolidar os riscos decorrentes da análise dos ambientes internos e externos que impactam o planejamento estratégico do TCE/TO;

II. Consolidar os riscos associados aos projetos, programas e portfólio da organização;

III. Disseminar e fornecer suporte metodológico à implantação e operacionalização do gerenciamento de riscos nas áreas técnicas do Tribunal de Contas do Estado do Tocantins.

VII. ASSESSORIA DE DESENVOLVIMENTO ORGANIZACIONAL

Compete à Assessoria de Desenvolvimento Organizacional:

I. Consolidar os riscos associados aos processos de negócios do Tribunal de Contas do Estado do Tocantins;

II. Disseminar e fornecer suporte metodológico para a implantação e operacionalização do gerenciamento de riscos nas áreas técnicas do TCETO.

VIII. CONSULTORIA JURÍDICA

Compete à Consultoria Jurídica/Diretoria Geral de Administração e Finanças:

I. Consolidar os riscos associados às aquisições de bens e serviços;

II. Disseminar e fornecer suporte metodológico para a implantação e operacionalização do gerenciamento de riscos nos processos de aquisições e prestação de serviços.

IX. GESTORES DE RISCOS

Compete aos gestores de riscos:

I. Executar as atividades relacionadas à gestão de riscos nos processos sob sua responsabilidade, identificando, gerenciando e tratando os riscos;

II. Monitorar a evolução dos riscos e avaliar a efetividade das medidas de controle implementadas nos processos sob sua gestão;

III. Definir as ações de tratamento de riscos, estabelecer prazos para implementação e avaliar os resultados alcançados;

IV. Propor medidas e ajustes nos controles a serem implementados no Sistema de Gestão de Riscos;

V. Comunicar a ocorrência de novos riscos que não estejam incluídos na relação de riscos institucionais;

VI. Elaborar, implementar, validar e revisar periodicamente a matriz de riscos em sua área de atuação;

VII. Conhecer e adotar a política, o manual e os instrumentos de gestão de riscos, promovendo a efetividade dos controles decorrentes desses instrumentos;

VIII. Reportar à chefia imediata quaisquer riscos que ultrapassem sua competência ou capacidade de gerenciamento;

São considerados gestores de riscos todas as chefias que atuam dentro de seus respectivos âmbitos e escopos de atuação.

X. INSTITUTO DE CONTAS 5 DE OUTUBRO

Compete ao Instituto de Contas 5 de Outubro:

I. Elaborar, implementar e monitorar programas de capacitação voltados à formação e atualização dos membros e servidores em temas relacionados à gestão de riscos, integridade, controles internos e governança, promovendo a disseminação de boas práticas institucionais.

II. Identificar necessidades de aprendizagem e desenvolver ações educacionais que fortaleçam as competências técnicas e comportamentais dos membros e servidores, com vistas ao fortalecimento da cultura de gestão de riscos e à promoção de uma atuação institucional eficiente e segura;

III. Conduzir campanhas, eventos e atividades de sensibilização que estimulem a conscientização, o comprometimento e o engajamento dos membros e servidores quanto à importância da gestão de riscos como instrumento de prevenção e aprimoramento da gestão pública.

XI. NÚCLEO DE CONTROLE INTERNO

Compete ao Núcleo de Controle Interno, por meio da Divisão de Auditoria Interna:

I. Fiscalizar o Sistema de Gestão de Riscos do TCETO, avaliando a adequação e eficácia dos mecanismos de gestão estabelecidos e a conformidade das atividades executadas, reportando à Presidência qualquer irregularidade ou ilegalidade;

II. Avaliar se o plano de gestão de riscos está em conformidade com a política estabelecida;

III. Avaliar a eficácia dos controles internos implementados e propor ações corretivas para mitigar os riscos identificados;

IV. Monitorar a aderência das unidades organizacionais às diretrizes, metodologias e instrumentos estabelecidos no Sistema de Gestão de Riscos, promovendo ações corretivas e orientativas sempre que identificadas desconformidades ou fragilidades nos processos de identificação, avaliação, tratamento e monitoramento de riscos.

XII. DIRETORIA GERAL DE CONTROLE EXTERNO

Compete à Diretoria Geral de Controle Externo:

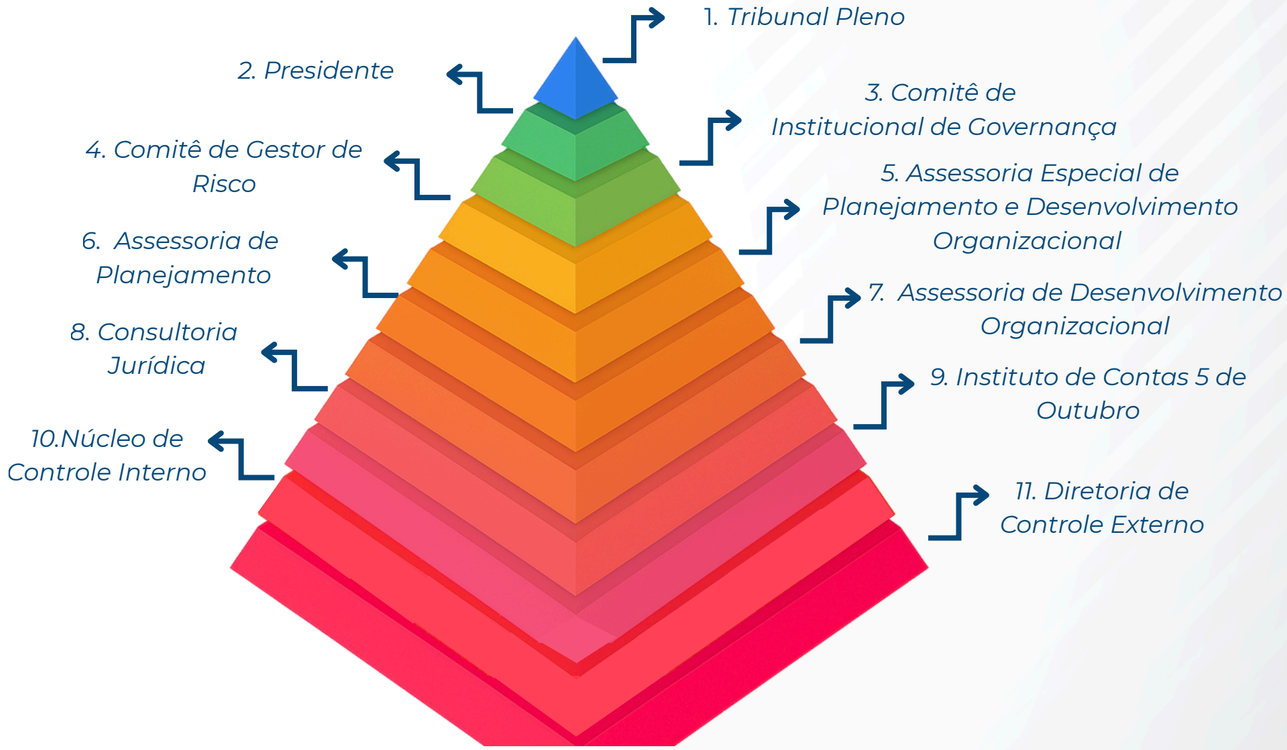
I. Avaliar a eficácia do sistema de gestão de riscos, controles internos e governança, por meio de ações de fiscalização, com o objetivo de examinar, de forma independente, a eficácia dos mecanismos de governança e gestão de riscos, bem como a conformidade e a aderência das práticas institucionais aos normativos vigentes;

II. Atuar com independência funcional e técnica na fiscalização da atuação das unidades responsáveis pela execução operacional (1ª linha) e pelo monitoramento e suporte à gestão de riscos (2ª linha), assegurando integridade, transparência e efetividade nos processos de controle;

III. Contribuir, a partir das constatações e análises realizadas, para o aprimoramento das práticas de governança, reforçando a *accountability*, a conformidade legal e a gestão estratégica de riscos no âmbito do Tribunal.

Conforme ilustrado na Figura 4, este conjunto de atribuições e responsabilidades garante que o Sistema de Gestão de Riscos e Continuidade do Negócio do TCETO seja eficaz, dinâmico e alinhado às melhores práticas de governança e gestão pública, assegurando a transparência, a eficiência e a segurança institucional.

Figura 4: Instâncias do Sistema de gestão de riscos do TCETO



8 Modelo de três linhas

O Modelo das Três Linhas surgiu há mais de duas décadas, consolidando-se como uma estrutura de referência internacionalmente reconhecida para o fortalecimento da governança, do gerenciamento de riscos e dos controles internos nas organizações. Sua formalização ocorreu em 2013, com a publicação da Declaração de Posicionamento “As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles”, pelo *The Institute of Internal Auditors* (IIA), conforme ilustrado na Figura 5. Esse documento contribuiu de forma significativa para a padronização conceitual dos papéis desempenhados pelas diferentes áreas organizacionais no contexto do gerenciamento de riscos.

Em 2020, o IIA promoveu uma revisão conceitual substancial do modelo, incorporando contribuições de especialistas e grupos de estudo em governança e gestão de riscos. A atualização resultou no reposicionamento da estrutura, que passou a ser denominada apenas “O Modelo das Três Linhas”. A exclusão do termo “defesa” teve como objetivo enfatizar a cooperação, a criação de valor organizacional e a interdependência entre os papéis de governança, gestão e auditoria interna.

No âmbito da administração pública, a adoção do Modelo das Três Linhas tem sido fortemente recomendada como prática de governança, visando ao aprimoramento da transparência, da responsabilização e da prestação de contas.

A estrutura fornece um arcabouço conceitual claro e acessível, capaz de fortalecer a comunicação institucional e de promover maior conscientização quanto às responsabilidades específicas de cada unidade organizacional no gerenciamento de riscos e nos controles internos.

Figura 5: Modelo de três linhas

O modelo também delineia as atribuições de cada área, contribuindo para a eliminação de ambiguidades, lacunas ou sobreposições na definição de responsabilidades relativas às atividades de gestão de riscos e de controles internos. Além disso, ressalta a importância da atuação da auditoria externa e dos órgãos reguladores como mecanismos complementares de controle.

Corpo Administrativo

Representado pela Alta Administração, é responsável por estabelecer a visão, a missão, os valores e o apetite ao risco institucional. Compete a esse corpo delegar à gestão a responsabilidade pela consecução dos objetivos organizacionais, bem como assegurar a provisão dos recursos necessários. Também lhe cabe receber relatórios gerenciais sobre os resultados planejados, realizados e esperados, assim como informações relacionadas à identificação e mitigação de riscos.

Primeira Linha

Compreende as unidades de gestão diretamente responsáveis pela entrega de produtos e serviços aos usuários ou clientes da organização. Inclui, ainda, as funções de apoio, mantendo diálogo constante com o corpo administrativo. Cabe-lhe reportar os resultados planejados, realizados e projetados, garantindo o alinhamento com os objetivos organizacionais, além do cumprimento das exigências legais, regulatórias e éticas.

Segunda Linha

Engloba as áreas encarregadas de oferecer suporte especializado ao gerenciamento de riscos, por meio de assessoramento técnico, monitoramento, revisão crítica e orientação. Atua no desenvolvimento, implementação e aprimoramento contínuo das práticas de gestão de riscos em todos os níveis da organização, fornecendo análises e relatórios sobre a adequação e a eficácia dos mecanismos de controle.

Terceira Linha

Representada pela Auditoria Interna, atua com independência em relação à gestão, prestando contas diretamente ao corpo administrativo. Sua função consiste em avaliar, de forma isenta e objetiva, a eficácia da governança, da gestão de riscos e dos controles internos, contribuindo para o alcance dos objetivos organizacionais e para a promoção da melhoria contínua. Compete-lhe, ainda, comunicar qualquer comprometimento de sua independência ou objetividade, adotando salvaguardas apropriadas quando necessário.

O Modelo das Três Linhas constitui-se, portanto, em uma estrutura sólida e adaptável, que promove maior clareza na distribuição de responsabilidades e fortalece a integração entre governança, gestão e auditoria interna. Ao ser implementado no setor público, torna-se instrumento estratégico para assegurar transparência, responsabilidade e eficiência administrativa, contribuindo, de forma decisiva, para a confiança da sociedade nas instituições.

9 Modelo de três linhas no TCETO

Na estrutura do Tribunal a estrutura de três linhas funciona da seguinte forma, conforme ilustrado na Figura 6.

Corpo Administrativo: representado pelo Tribunal Pleno, o Comitê Institucional de Governança e o Comitê Gestor de Risco, com o papel de direcionar, monitorar e avaliar o atingimento dos objetivos do sistema de gestão de riscos do TCETO, por meio de relatórios, apoiando e fornecendo os recursos necessários.

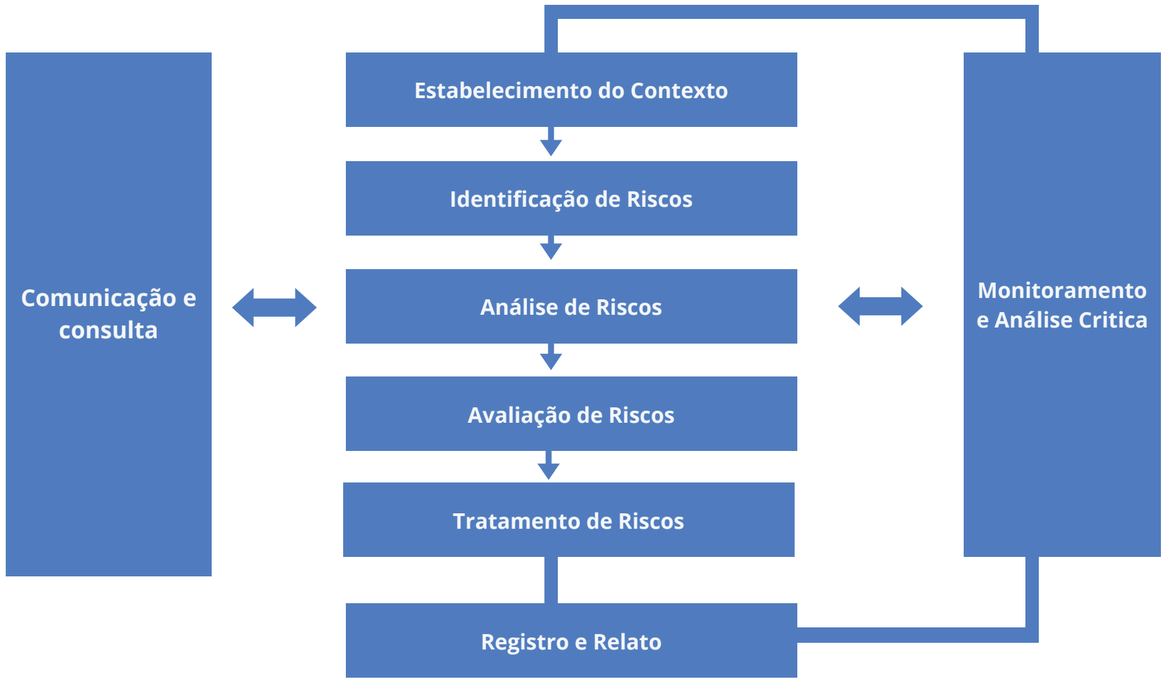
- **Primeira Linha:** representado pelas unidades e gestores de riscos do Tribunal, devendo executar em conformidade as ações de gerenciamento de riscos;
- **Segunda Linha:** Compreende as áreas ASPDO, ASPLA, ASSDO, e Consultoria Jurídica responsáveis por oferecer suporte especializado ao gerenciamento de riscos, por meio de assessoramento técnico, monitoramento, revisão crítica e orientação. Atuam no desenvolvimento, implementação e aprimoramento contínuo das práticas de gestão de riscos em todos os níveis – processos, sistemas e estrutura organizacional.
- **Terceira Linha:** representada pelo Núcleo de Controle Interno; deve prestar contas perante o corpo administrativo de forma independente, avaliando o sistema de gestão de riscos, reportando ao corpo administrativo quaisquer prejuízos à independência e objetividade e implantando salvaguardas conforme necessário.

Figura 6: Modelo de três linhas do TCETO

10 Processo de gestão de riscos

O processo de gestão de riscos no Tribunal de Contas do Estado de Tocantins (TCETO), conforme ilustrado na Figura 7, abrange as seguintes etapas: o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento de riscos, o registro e relato, a comunicação e consulta com as partes interessadas, o monitoramento e a análise crítica.

Figura 7 : Processo de gestão de riscos do TCETO



ESTABELECIMENTO DO CONTEXTO

O estabelecimento do contexto envolve o levantamento e registro dos fatores internos e externos que são cruciais para alcançar os objetivos institucionais. Seu propósito é proporcionar uma compreensão clara do ambiente no qual a organização está inserida, além de identificar os fatores que podem impactar a capacidade da organização de atingir os resultados planejados.

A análise do ambiente visa reunir informações que apoiem a identificação de riscos e subsidiem a escolha de ações adequadas para assegurar o alcance dos objetivos organizacionais.

No que tange ao ambiente interno, é essencial examinar elementos relacionados à integridade, aos valores éticos, à competência das equipes, à estrutura de governança do Tribunal, bem como às políticas e práticas implementadas.

11 Estabelecimento do Contexto

Em relação ao ambiente externo, deve-se considerar os fatores que estão além do controle direto da organização, mas que podem influenciar seu desempenho.

Estes incluem aspectos econômicos, políticos, sociais, tecnológicos e legais, que podem criar oportunidades ou representar ameaças. A compreensão dessas variáveis é fundamental para a organização se adaptar e planejar estratégias adequadas para lidar com as mudanças e desafios que surgem no cenário externo.

No que diz respeito à fixação de objetivos, é necessário verificar, em todos os níveis (processo, projeto, aquisição e atividades), se os objetivos foram estabelecidos e comunicados de forma eficaz, e se estão alinhados com a missão e visão do Tribunal.

Após essas definições, deve-se registrar o objetivo geral do processo, projeto ou aquisição. Essas informações devem estar em conformidade com a cadeia de valor da instituição e com o mapeamento de processos existentes.

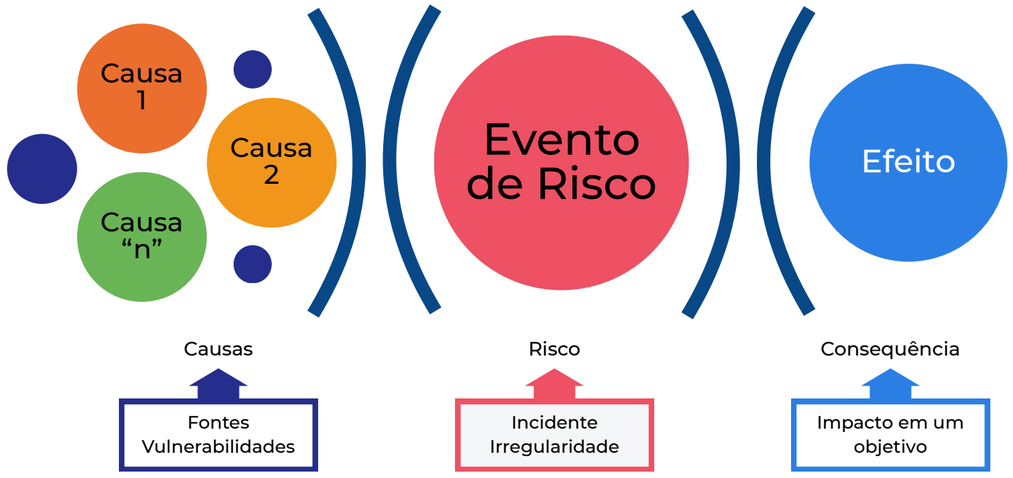
Uma ferramenta importante para apoiar essa etapa da gestão de riscos é a análise SWOT, que permite identificar as forças, fraquezas do ambiente interno, bem como as oportunidades e ameaças do ambiente externo, conforme ilustrado na Figura 8. Recomenda-se a utilização da técnica brainstorming, por favorecer o surgimento de informações e ideias quanto ao contexto.

Figura 8 : Análise SWOT

12 Identificação dos riscos

A etapa de identificação de riscos consiste no reconhecimento, descrição e registro dos eventos de risco, contemplando a caracterização de suas prováveis causas e potenciais consequências. Um mesmo evento pode ter múltiplas causas e gerar diferentes impactos, conforme ilustrado na Figura 9. Para assegurar a qualidade dessa fase, é imprescindível a participação de pessoas que detenham conhecimento técnico e experiência adequada. Nessa etapa, elabora-se uma lista de eventos que possam comprometer os resultados organizacionais, dificultar o alcance dos objetivos e, em última instância, afetar o valor público a ser entregue à sociedade. Ressalta-se, ainda, a relevância das informações provenientes da etapa anterior do processo de gestão de riscos.

Figura 9 - Identificação dos riscos.

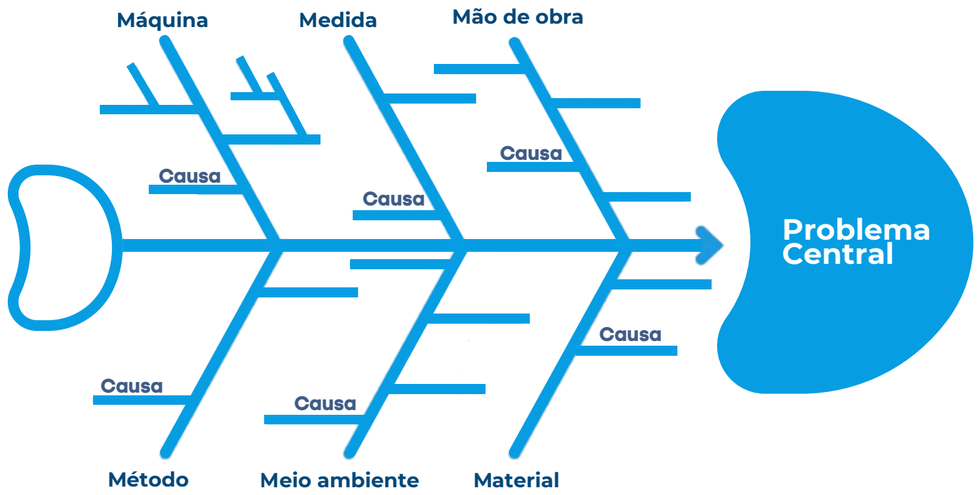


A descrição dos riscos deve oferecer uma visão abrangente acerca do que pode falhar em determinado processo, projeto ou aquisição. Para orientar essa análise, algumas questões são úteis: o que pode dar errado; quais ativos estão em risco (recursos, informações, reputação, legalidade); de onde se originam os riscos; a quem se vinculam; e quais fatores podem limitar o desempenho do programa ou processo.

Após a definição dos riscos, torna-se necessário identificar suas causas e consequências potenciais. Diversas técnicas podem ser empregadas para esse fim, como brainstorming, diagrama de Ishikawa, método Bow-Tie, entrevistas com especialistas e análise de cenários.

O Diagrama de Ishikawa, conforme ilustrado na Figura 10, também conhecido como diagrama de causa e efeito ou diagrama espinha de peixe, é uma ferramenta utilizada para identificar, organizar e representar graficamente as possíveis causas de um problema ou evento de risco. Sua estrutura visual assemelha-se ao formato de uma espinha de peixe, em que o "efeito" ou problema identificado ocupa a posição da "cabeça", enquanto as principais categorias de causas, normalmente agrupadas em fatores como processos, pessoas, materiais, equipamentos, ambiente e métodos, formam as "espinhas".

Figura 10 - Diagrama de Ishikawa (causa e efeito)

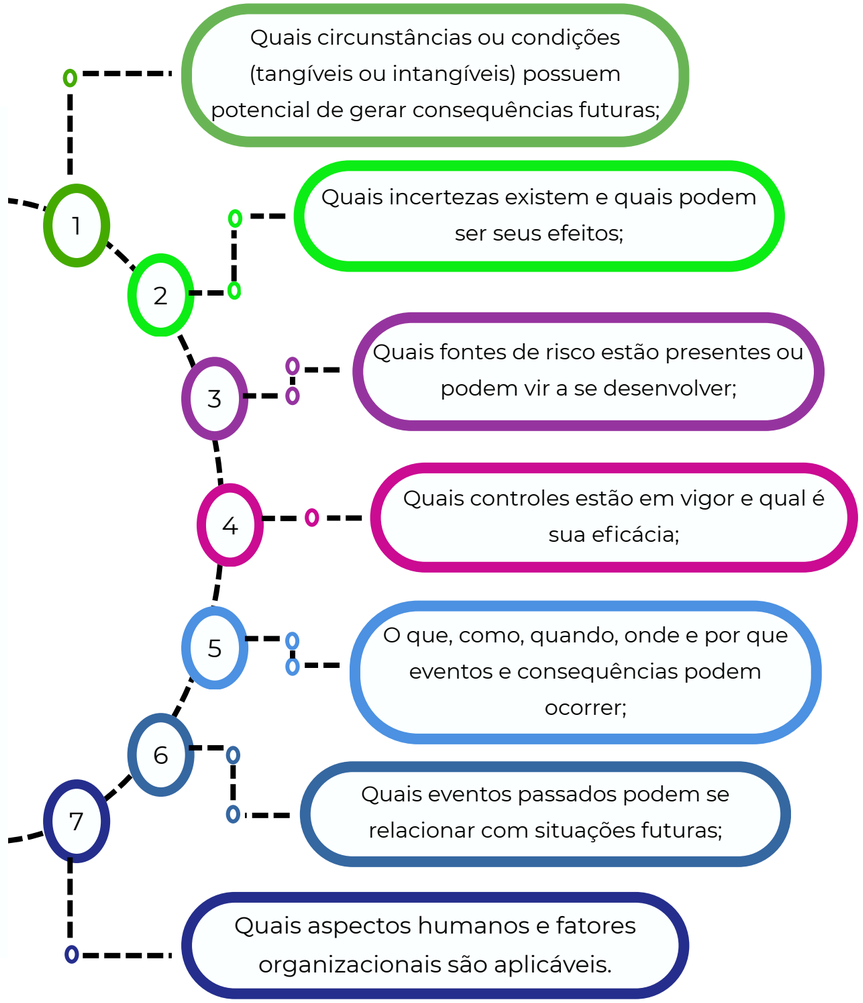


Na identificação de riscos, devem ser considerados fatores relacionados à infraestrutura, pessoal, tecnologia e processos, além da regulamentação interna e externa. Igualmente relevantes são o conhecimento organizacional, os relatórios gerenciais que evidenciem situações de risco potencial ou inerente, bem como os relatórios de auditoria interna e externa.

A atividade de identificação pode ser realizada em oficinas de trabalho ou, conforme o caso, pelo próprio gestor do risco. É essencial que as equipes encarregadas dessa etapa possuam visão holística das competências institucionais e dos processos de trabalho em seus diferentes níveis.

As técnicas empregadas para a identificação de riscos geralmente se valem do conhecimento e da experiência de uma ampla gama de partes interessadas. Nessa fase, conforme apresentado na figura 11, recomenda-se considerar:

Figura 11 - Considerações acerca das técnicas de identificação de risco



De modo geral, o risco encontra-se associado a uma causa e a uma consequência:

- Causa (o quê e por quê): geralmente uma combinação de causas diretas e intrínsecas que levam à ocorrência do evento;
- Consequência: resultado ou impacto que o risco ocasiona sobre os objetivos da organização.

A seguinte sintaxe, utilizada para a descrição de aspectos relacionados a um evento de risco, contribui para a reflexão e o aprimoramento desta etapa.

Devido a **< CAUSA, FONTE >**, poderá acontecer **< EVENTO DE RISCO>**, o que poderá levar a **< IMPACTO, EFEITO, CONSEQUÊNCIA >**, levando o não atingimento do **< OBJETIVO >**

Após a definição do(s) risco(s), bem como de suas respectivas causas e consequências, é necessário proceder à sua classificação, conforme as categorias:

- **Operacional**: eventos que podem comprometer as atividades da unidade, usualmente associados a falhas, deficiências ou inadequações em processos internos, recursos humanos, infraestrutura ou sistemas. Tais eventos afetam diretamente a eficácia e a eficiência da gestão dos processos organizacionais;

- **Orçamentária**: eventos que podem comprometer a capacidade da unidade de dispor dos recursos orçamentários necessários à execução de suas atividades ou ainda, que possam prejudicar a própria execução orçamentária;

- **Reputacional**: eventos que podem abalar a confiança da sociedade na capacidade da unidade de cumprir sua missão institucional, impactando negativamente a imagem do órgão;

- **Fiscal**: eventos que possam afetar de forma adversa o equilíbrio das contas públicas;

- **Conformidade**: eventos que possam comprometer a observância de leis, normas e regulamentos aplicáveis;

- **Social**: eventos que podem afetar negativamente o valor público percebido ou esperado pela sociedade em relação aos resultados decorrentes da prestação dos serviços públicos pela instituição;

- **Integridade**: eventos relacionados à ocorrência de corrupção, fraudes, irregularidades e/ou desvios éticos ou de conduta, que possam comprometer os valores institucionais do Tribunal e a consecução de seus objetivos

Na hipótese de um mesmo evento de risco se enquadrar em duas ou mais categorias, deverá ser escolhida aquela que melhor represente o aspecto mais relevante quanto ao impacto que tal evento poderá ocasionar, caso venha a se concretizar. A saída dessa etapa corresponde a uma lista estruturada de riscos, contemplando a descrição dos eventos, suas causas e suas consequências.

13 Análise de riscos

O propósito da análise de riscos é compreender a natureza dos riscos identificados, bem como suas principais características, incluindo o respectivo nível de risco. Trata-se de uma etapa que envolve a consideração detalhada de incertezas, fontes geradoras de risco, consequências potenciais, probabilidades de ocorrência, eventos e cenários, além da análise dos controles internos existentes e de sua eficácia.

Cabe destacar que um único evento pode ter múltiplas causas e consequências, podendo afetar diversos objetivos institucionais simultaneamente. A análise de riscos pode ser realizada com diferentes níveis de profundidade e complexidade, a depender do objetivo da análise, da disponibilidade e confiabilidade das informações, bem como dos recursos técnicos e operacionais disponíveis.

A análise do risco inerente deve considerar, prioritariamente, a probabilidade de ocorrência do evento, com base em uma abordagem qualitativa e, sempre que possível, complementada por dados quantitativos. Essa análise deve estar fundamentada no conhecimento técnico e na experiência dos profissionais envolvidos no processo, podendo ainda ser enriquecida por informações estatísticas, registros de eventos anteriores e médias históricas.

A conjugação de distintas fontes de informação, como experiências anteriores, tendências setoriais e alterações no ambiente regulatório, contribui para uma compreensão mais ampla e precisa do cenário de risco, permitindo avaliações mais robustas e fundamentadas. Essa abordagem integrada favorece a identificação de eventuais lacunas na análise e a definição de estratégias mais eficazes para o gerenciamento dos riscos.

Considerando que todos os riscos foram previamente documentados na etapa de identificação, torna-se imprescindível realizar uma avaliação minuciosa de cada um deles, utilizando-se, para tanto, as escalas de probabilidade e impacto.

A avaliação da probabilidade de ocorrência de um evento de risco constitui uma etapa essencial na análise de riscos, pois permite estimar a chance de materialização do evento com base em critérios sistemáticos e padronizados. Conforme ilustrado na Figura 12, essa estimativa é realizada por meio de uma escala ordinal que varia entre os seguintes níveis: muito rara, pouco provável, provável, muito provável e praticamente certa. A utilização dessa escala visa conferir maior objetividade e uniformidade ao processo avaliativo, facilitando a comparação entre diferentes riscos e contribuindo para a priorização daqueles que demandam atenção mais imediata.

Além disso, a definição do nível de probabilidade deve considerar não apenas a experiência dos especialistas envolvidos, mas também dados históricos, estatísticas disponíveis e qualquer outra evidência que possa sustentar tecnicamente a estimativa realizada.

Figura 12: Matriz de probabilidade.

Escala de Probabilidade			
Peso	**Descrição**	**Aspecto Avaliativo**	**Frequência observada/ esperada**
5	Praticamente Certo	Ocorrência quase garantida no prazo associado ao objetivo; evento com altíssima probabilidade de ocorrência	> 80%
4	Muito Provável	Repete-se com elevada frequência no prazo associado ao objetivo, ou há muitos indícios que ocorrerá nesse horizonte; evento deve ocorrer na maioria das circunstâncias	> 60% e ≤ 80%
3	Provável	Repete-se com frequência razoável no prazo associado ao objetivo, ou há indícios que possa ocorrer nesse horizonte; evento deve ocorrer em algum momento	> 40% e ≤ 60%
2	Pouco Provável	O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo; evento pode ocorrer em algum momento	> 20% e ≤ 40%
1	Rara	Não há histórico conhecido do evento, ou não há indícios que sinalizem sua ocorrência; evento que acontece apenas em situações excepcionais.	≤ 20%

Dessa forma, a avaliação da probabilidade torna-se um instrumento decisivo para a construção de uma matriz de risco consistente e eficaz.

Já a avaliação do impacto representa uma etapa crucial no processo de gestão de riscos, pois permite mensurar, de forma estruturada, as possíveis consequências decorrentes da concretização de um evento adverso. Essa mensuração é realizada com base no grau de comprometimento que o risco poderá causar aos objetivos institucionais, considerando seus efeitos sobre os processos, os resultados esperados e os recursos críticos da organização.

Essa mensuração é realizada com base na análise das consequências potenciais do evento, considerando a gravidade dos efeitos sobre os processos, os resultados esperados, os recursos disponíveis e demais elementos críticos ao alcance das metas organizacionais. Assim, a escala de impacto contribui para a classificação e priorização dos riscos, permitindo à gestão tomar decisões mais embasadas quanto à necessidade de tratamento, monitoramento ou aceitação dos riscos identificados.

Para orientar essa análise, utiliza-se a escala de impacto, instrumento que confere uniformidade à avaliação e facilita a classificação dos riscos conforme sua severidade. Tal escala contempla os seguintes níveis: muito baixo, baixo, médio, alto e muito alto, graduando o impacto em relação ao comprometimento dos objetivos organizacionais. A definição do nível de impacto deve considerar não apenas a gravidade das consequências potenciais, mas também a sua abrangência e a capacidade da instituição de responder aos efeitos do evento.

Conforme ilustrado na Figura 13, a aplicação consistente dessa escala contribui significativamente para a priorização dos riscos e para a tomada de decisões mais embasadas quanto às medidas de tratamento, monitoramento ou aceitação a serem adotadas.

Figura 13: Matriz de impacto.

Escala de Impacto			
Peso	**Descrição**	**Aspecto Avaliativo**	**Frequência observada/ esperada**
5	Muito Alto	Compromete totalmente ou quase totalmente o atingimento do objetivo.	> 80%
4	Alto	Compromete a maior parte do atingimento do objetivo.	> 60% e ≤ 80%
3	Médio	Compromete o alcance do objetivo.	> 40% e ≤ 60%
2	Baixo	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo.	> 20% e ≤ 40%
1	Muito Baixo	Compromete minimamente o atingimento do objetivo, para fins práticos, não altera o alcance do objetivo.	≤ 20%

É recomendável que a consistência das percepções relativas à probabilidade e ao impacto seja devidamente respaldada pelo registro de evidências substanciais, tais como dados, documentos, relatórios e arquivos constantes em sistemas.

A multiplicação dos valores atribuídos à probabilidade e ao impacto resulta no risco inerente:

NÍVEL DO RISCO INERENTE = **PROBABILIDADE** X **IMPACTO**

O resultado do risco inerente é classificado em um dos quatro níveis da Matriz de Risco: Baixo(entre 1 a 4), Médio(entre 5 e 14), Alto (entre 15 e 24) e Extremo (25), conforme ilustrado na Figura 14.

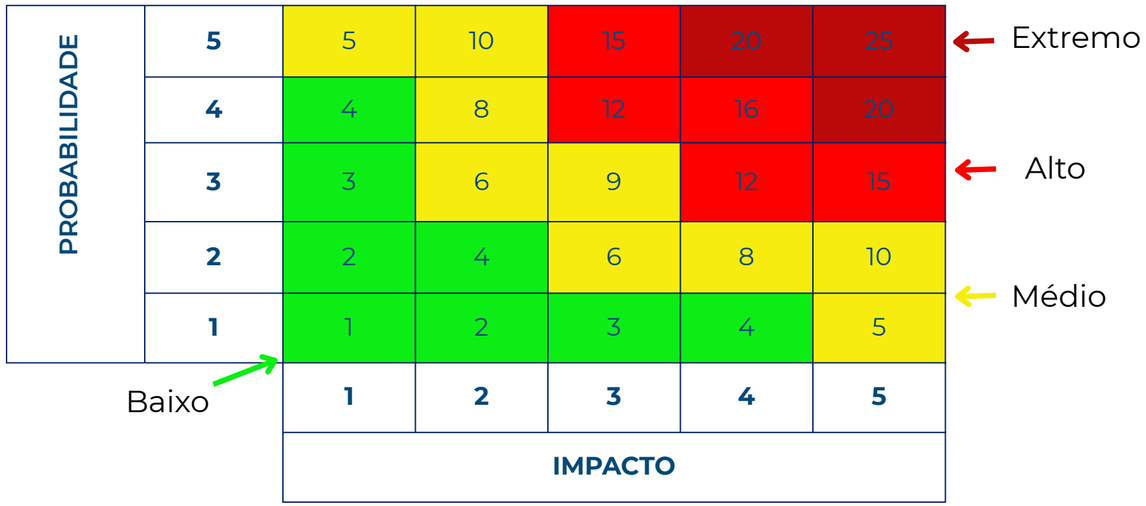
Figura 14 : Matriz de riscos.

Nível do risco	Faixa
Baixo	1-4
Médio	5-11
Alto	12-19
Extremo	20-25

Se um determinado risco foi avaliado com níveis de probabilidade provável (3) e nível de impacto muito alto (5), terá como nível de risco inerente 15, desta forma será classificado como risco alto.

Após encontrar o resultado do cálculo, o risco pode ser identificado dentro das seguintes faixas elencadas na Figura 15:

Figura 15 : Matriz de probabilidade x impacto.



Após a análise do risco inerente (sem considerar controles existentes), deve identificar a existência dos controles internos e realizar a avaliação da eficácia quanto a operação do controle.

No âmbito da gestão de riscos organizacionais, a identificação e a avaliação do risco inerente, ou seja, aquele que subsiste na ausência de quaisquer mecanismos de mitigação representam uma etapa fundamental para a compreensão plena das ameaças às quais a entidade está exposta. Todavia, essa análise não deve se encerrar com a constatação do risco em seu estado bruto. É imperativo, na sequência, proceder à identificação dos controles internos existentes que tenham como finalidade mitigar tais riscos.

A identificação dos controles internos, conforme ilustrado na Figura 16, compreende o reconhecimento das políticas, procedimentos, práticas e estruturas implementadas pela organização com o objetivo de assegurar a consecução de seus objetivos, proteger ativos, assegurar a integridade das informações e o cumprimento de normas e regulamentos. Estes controles podem ser de natureza preventiva, detectiva ou corretiva, e devem estar diretamente correlacionados ao risco previamente identificado.

Figura 16 : Verificação de controle internos implementados.

Avaliação quanto a existência do controle	
1	Não há procedimento de controle.
2	Há procedimentos de controles, mas não são adequados e nem estão formalizados;
3	Há procedimentos de controles formalizados, mas não estão adequados (insuficientes);
4	Há procedimentos de controles adequados (suficientes), mas não estão formalizados;
5	Há procedimentos de controles adequados (suficientes) e formalizados.

Posteriormente à identificação dos controles, impõe-se a realização de uma avaliação criteriosa quanto à eficácia de sua operação, conforme ilustrado na Figura 17. Tal análise deve considerar se os controles estão adequadamente desenhados, implementados e, sobretudo, se operam de maneira contínua e eficaz no contexto operacional da organização. Uma avaliação eficaz deve ser pautada em evidências concretas, podendo envolver testes de controle, entrevistas com responsáveis, revisão documental e observação direta das práticas executadas.

Figura 17 : Avaliação do funcionamento do controle.

Avaliação quanto a operação do controle	
1	Não há procedimentos de controle.
2	Há procedimentos de controle, mas não são executados.
3	Há procedimento de controle, mas são parcialmente executados.
4	Há procedimento de controles executados, mas sem evidência de sua realização.
5	Há procedimento de controle executados e com evidência de sua realização.

A compreensão clara da eficácia operacional dos controles permite à organização determinar o risco residual, ou seja, aquele que persiste mesmo após a atuação dos mecanismos de controle. Essa avaliação é essencial para subsidiar decisões estratégicas quanto à necessidade de aprimoramento dos controles existentes ou à implementação de novos dispositivos de mitigação.

Posteriormente à identificação dos controles, impõe-se a realização de uma avaliação criteriosa quanto à eficácia de sua operação, conforme ilustrado na Figura 18.

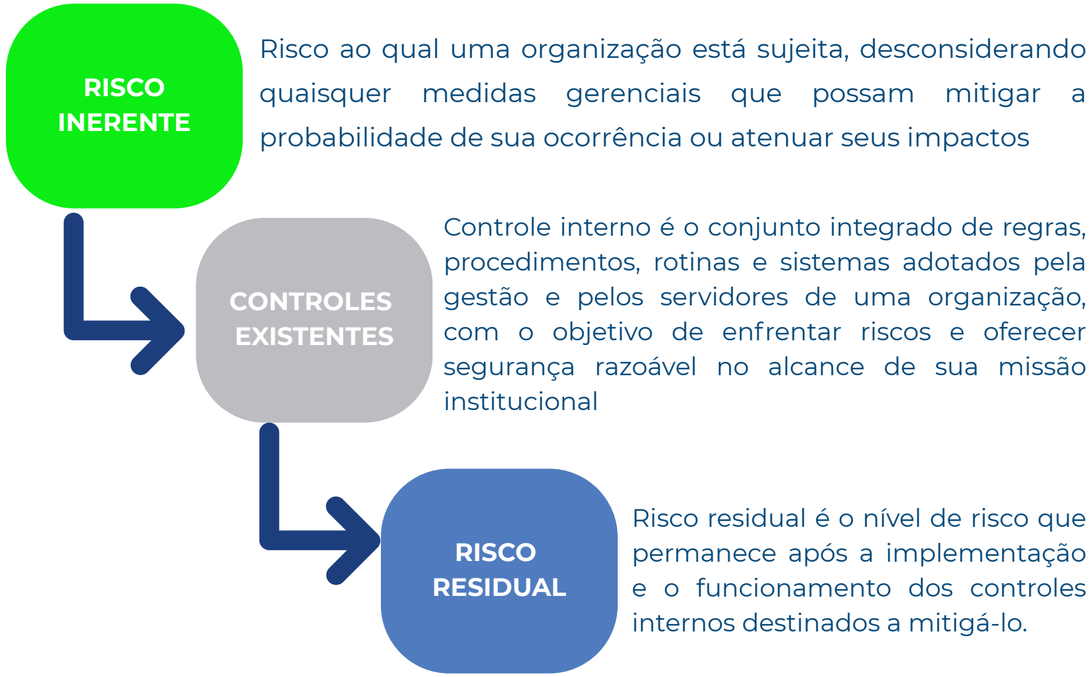
Figura 18 : Avaliação da efetividade do controle.

Avaliação do controle	
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.
Fraco	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco

Tal análise deve considerar se os controles estão adequadamente desenhados, implementados e, sobretudo, se operam de maneira contínua e eficaz no contexto operacional da organização. Uma avaliação eficaz deve ser pautada em evidências concretas, podendo envolver testes de controle, entrevistas com responsáveis, revisão documental e observação direta das práticas executadas

A compreensão clara da eficácia operacional dos controles permite à organização determinar o risco residual, ou seja, aquele que persiste mesmo após a atuação dos mecanismos de controle. Essa avaliação é essencial para subsidiar decisões estratégicas quanto à necessidade de aprimoramento dos controles existentes ou à implementação de novos dispositivos de mitigação, conforme demonstrado na Figura 19.

Figura 19 : Ciclo do gerenciamento de risco.



Após avaliar a eficácia dos controles existentes, deve-se aferir o nível de risco residual, indicando os novos pesos relativos à probabilidade e ao impacto. Multiplicando-se esses pesos, obteremos o valor do risco residual e em qual nível da Matriz de Apetite a Risco ele estará inserido, observando as ações a serem adotadas para cada nível de risco, conforme ilustrado na Figura 20.

Figura 20 : Matriz de probabilidade x impacto.

PROBABILIDADE						
	5 Praticamente certo	5	10	15	20	25
	4 Muito Provável	4	8	12	16	20
	3 Provável	3	6	9	12	15
	2 Pouco Provável	2	4	6	8	10
	1 Rara	1	2	3	4	5
		1 Muito Baixo	**2** Baixo	**3** Médio	**4** Alto	**5** Muito Alto
		IMPACTO				

14 Avaliação de riscos

A avaliação de riscos constitui uma etapa essencial no processo de gestão de riscos, tendo como principal finalidade subsidiar a tomada de decisões de forma criteriosa, fundamentada e alinhada aos objetivos organizacionais. Essa fase deve ser conduzida pelo gestor de riscos e compreende a comparação entre os resultados obtidos na análise de riscos e os critérios previamente estabelecidos pela instituição, com o propósito de determinar a necessidade de adoção de medidas adicionais. Ressalta-se que essa comparação deve considerar o risco residual, ou seja, aquele que permanece após a aplicação dos controles internos já existentes e efetivamente implementados, os quais possuem a capacidade de mitigar o risco inerente previamente identificado.

O nível de risco identificado deve ser confrontado com os critérios definidos pela organização, especialmente no que tange ao seu apetite ao risco. Tal comparação é indispensável para verificar se o risco é aceitável ou se demanda a implementação de ações de tratamento.

Entende-se por apetite ao risco o grau de exposição a riscos que a organização está disposta a aceitar na busca pela consecução de seus objetivos estratégicos. Esse parâmetro serve como referência para decisões consistentes e alinhadas à tolerância institucional às incertezas.

No âmbito do Tribunal de Contas, o apetite ao risco está formalmente definido em sua Declaração de Apetite ao Risco, a qual orienta as decisões relacionadas à aceitação ou ao tratamento de riscos identificados.

Com base nessa avaliação, diversas decisões podem ser adotadas, tais como: a manutenção do status quo, ou seja, a não adoção de medidas adicionais; a consideração de alternativas para o tratamento dos riscos identificados; a realização de análises complementares com vistas a uma compreensão mais aprofundada do risco; a preservação dos controles atualmente em vigor; ou, ainda, a reavaliação dos objetivos organizacionais à luz dos riscos mapeados.

É recomendável que essas decisões considerem o contexto organizacional mais amplo, incluindo os impactos reais e percebidos sobre as partes interessadas, internas e externas. Essa abordagem integrada contribui para a construção de decisões mais coerentes com os valores institucionais, a missão e os objetivos estratégicos da organização.

Por fim, os resultados da avaliação de riscos devem ser formalmente registrados, comunicados e validados nos níveis apropriados da estrutura organizacional, a fim de assegurar a transparência, a rastreabilidade e a legitimidade do processo decisório.

15 Tratamento de riscos

A etapa de tratamento de riscos constitui uma fase essencial no processo de gestão de riscos, principal selecionar e implementar as opções mais adequadas para lidar com os riscos identificados, sejam eles ameaças, que podem comprometer o alcance dos objetivos, ou oportunidades, que podem favorecê-los.

Nesse sentido, o tratamento de riscos visa reduzir a probabilidade de ocorrência ou o impacto das ameaças, bem como aumentar a probabilidade de ocorrência ou o impacto das oportunidades.

Trata-se de um processo iterativo, composto pelas seguintes atividades fundamentais:

- Formulação e seleção de opções de tratamento do risco: nesta etapa, são analisadas as alternativas disponíveis para lidar com cada risco, considerando sua natureza (ameaça ou oportunidade) e sua viabilidade técnica, econômica e organizacional. No caso das ameaças, buscam-se estratégias que reduzam sua probabilidade ou impacto. Já no caso das oportunidades, priorizam-se ações que aumentem a chance de sua concretização ou ampliem seus efeitos positivos.

- Planejamento e implementação do tratamento: Após a seleção das opções mais adequadas, deve-se elaborar um plano de ação claro, que inclua prazos definidos, responsáveis designados e os recursos necessários à execução das medidas propostas, seja para conter ameaças, seja para fomentar oportunidades.

- Avaliação da eficácia do tratamento: As ações implementadas devem ser avaliadas quanto à sua efetividade na modificação dos riscos. No caso das ameaças, verifica-se se as medidas adotadas estão sendo eficazes na redução da probabilidade de ocorrência ou do impacto do risco. Já em relação às oportunidades, avalia-se se as ações estão promovendo, de forma satisfatória, o aproveitamento dos benefícios potenciais identificados. Essa avaliação contínua permite o ajuste das estratégias sempre que necessário, com o objetivo de maximizar os resultados positivos e mitigar eventuais efeitos indesejados.

- Decisão quanto à aceitabilidade do risco remanescente: a organização deve verificar se o risco residual, ou seja, aquele que permanece após a aplicação das medidas de tratamento, é aceitável à luz de seus objetivos estratégicos e do apetite ao risco estabelecido. No caso das ameaças, essa decisão envolve a aceitação de um nível de risco controlado.

Para oportunidades, pode significar a manutenção do risco com expectativa de ganho, ainda que não esteja totalmente controlado.

Tratamento adicional (se necessário): Caso o risco remanescente seja considerado inaceitável, seja pelo potencial de dano, no caso de ameaças, ou pela insuficiência de aproveitamento, no caso de oportunidades, devem ser avaliadas e implementadas medidas complementares.

Figura 21 : Opções de tratamento de riscos com impacto negativo.

A seleção das opções de tratamento requer uma análise criteriosa dos benefícios esperados em comparação com os custos, os esforços e os possíveis efeitos adversos associados à sua implementação. Ressalta-se que as opções de tratamento não são, necessariamente, excludentes entre si, podendo ser adotadas de forma combinada, conforme o contexto.

As alternativas de tratamento de riscos podem incluir, entre outras, aquelas ilustradas na figura 21.

Cumpre destacar que cada gestor de riscos é responsável pela condução do tratamento dos riscos sob sua responsabilidade, incumbindo-lhe a definição das estratégias mais adequadas, tanto para mitigar ameaças quanto para promover oportunidades, o acompanhamento da execução das ações e a comunicação com as partes interessadas envolvidas. Essa abordagem descentralizada confere maior agilidade ao processo, assegura coerência técnica e favorece o alinhamento com as particularidades de cada área.

Todavia, nos casos em que os riscos ultrapassarem o apetite da organização, seja por apresentarem ameaças inaceitáveis ou por representarem oportunidades que demandem investimentos ou decisões estratégicas, o plano de tratamento deverá ser submetido à apreciação do Comitê Gestor de Riscos, com vistas ao monitoramento de sua implementação e da eficácia das ações propostas, e posteriormente deliberação pelo Presidente.

Mesmo com um planejamento criterioso, o tratamento de riscos pode não gerar os resultados esperados ou, ainda, produzir efeitos não intencionais, inclusive o surgimento de novos riscos.

Por essa razão, o monitoramento contínuo e a análise crítica devem integrar o processo, assegurando a efetividade das medidas ao longo do tempo.

É Importante ressaltar que os riscos decorrentes do próprio processo de tratamento, também denominados riscos secundários, devem ser identificados, avaliados e formalmente incorporados ao plano de gerenciamento de riscos. Cabe ao gestor de riscos considerar esses efeitos colaterais como parte natural de um processo iterativo, que exige constante revisão e adaptação das estratégias adotadas.

A inclusão desses novos riscos no plano possibilita seu monitoramento e tratamento de forma proativa, evitando que comprometam os objetivos do projeto ou da organização.

Na ausência de opções viáveis de tratamento, ou quando estas se mostrarem insuficientes, recomenda-se que o risco, seja ameaça ou oportunidade, sejam registrado e mantido sob revisão contínua.

Nesses casos, os tomadores de decisão e as demais partes interessadas devem ser informados acerca da natureza e a extensão dos riscos remanescentes, que devem ser formalmente documentados, monitorados e, quando pertinente, submetidos a novo tratamento.

Para garantir clareza e controle sobre as ações a serem adotadas, o tratamento dos riscos deve ser formalizado por meio de um Plano de Tratamento de Riscos, que deve contemplar:

- a justificativa para a seleção das opções escolhidas, com destaque para os benefícios esperados;
- a designação dos responsáveis pela aprovação e implementação do plano;
- a descrição detalhada das ações a serem executadas;
- a especificação dos recursos necessários, incluindo provisões para contingências;
- a definição de métricas de desempenho para avaliação dos resultados;
- a identificação de eventuais restrições existentes.

Dessa forma, o tratamento de riscos envolve a elaboração e a implementação de um plano que estabeleça as medidas a serem adotadas, os controles a serem implementados ou aperfeiçoados, o cronograma de execução e os responsáveis por seu acompanhamento. Ao definir as estratégias de controle, o gestor deve considerar o apetite ao risco institucional, bem como os custos e benefícios associados a cada ação, tanto para a mitigação de ameaças quanto na promoção de oportunidades.

16 Registro e Relato

A etapa de Registro e Relato constitui parte essencial do processo de gerenciamento de riscos, sendo fundamental para assegurar a rastreabilidade, a transparência e a coerência das decisões tomadas ao longo do ciclo de vida do projeto. Esta etapa visa documentar, de forma adequada e sistemática, todas as informações relevantes relacionadas à identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos.

O registro deve abranger dados precisos e completos sobre os riscos identificados, os critérios adotados para sua avaliação, as decisões tomadas, as justificativas correspondentes, bem como os responsáveis por sua implementação e monitoramento. Este processo deve possibilitar o acompanhamento histórico das ações e servir como fonte de informação para auditorias, revisões críticas, análises comparativas e iniciativas de melhoria contínua.

O relato, por sua vez, refere-se à comunicação estruturada das informações registradas, de forma clara, tempestiva e dirigida aos públicos apropriados dentro da organização.

A comunicação deve ser proporcional à relevância dos riscos e alinhada aos níveis de autoridade e responsabilidade. Os relatos devem subsidiar a tomada de decisão em todos os níveis hierárquicos, promovendo a integração da gestão de riscos à governança, à gestão estratégica e à gestão de desempenho da instituição.

Convém que os registros e relatos sejam realizados de forma padronizada, em conformidade com as diretrizes institucionais e requisitos legais e regulatórios aplicáveis, assegurando a confidencialidade, a integridade e a acessibilidade das informações. A consistência desses documentos contribui para o fortalecimento da cultura organizacional voltada à gestão de riscos e à melhoria contínua dos processos.

Além disso, os resultados do registro e do relato devem retroalimentar o próprio sistema de gestão de riscos, apoiando o monitoramento, a análise crítica e a revisão da metodologia adotada, em consonância com os princípios da transparência, responsabilidade e melhoria contínua previstos na norma.

17 Comunicação e Consulta

A etapa de comunicação e consulta constitui um elemento transversal e indispensável do processo de gerenciamento de riscos. Sua finalidade é assegurar um fluxo contínuo, estruturado e eficaz de informações entre as partes interessadas, internas e externas à organização, promovendo o entendimento compartilhado dos riscos e o engajamento na formulação e implementação das medidas de tratamento.

O objetivo central dessa etapa é apoiar as partes interessadas na compreensão dos riscos, nos fundamentos que embasam a tomada de decisões e nas razões que justificam a adoção de ações específicas. Para tanto, exige-se a manutenção de um fluxo constante de comunicação, tanto informativa quanto consultiva, durante todas as fases do processo de gestão de riscos. Essa comunicação deve ser conduzida de maneira clara, objetiva e tempestiva.

Inicialmente, devem ser identificadas as partes interessadas, bem como levantadas suas necessidades e expectativas. A partir desse diagnóstico, deve-se elaborar o plano de comunicação e consulta, contemplando de forma sistemática todos os stakeholders.

Destaca-se que a comunicação deve abranger todas as fases do gerenciamento de riscos, desde a definição do contexto até o monitoramento e a análise crítica.

Assim, é imprescindível que se considerem as necessidades de informação dos diferentes públicos, de acordo com seus níveis de autoridade, responsabilidade e interesse. O conteúdo comunicado deve incluir, entre outros aspectos, a natureza dos riscos, suas causas e consequências potenciais, os critérios de avaliação utilizados, as decisões tomadas e as ações implementadas.

Compete ao gestor de riscos conduzir esse processo, assegurando que as informações sejam transmitidas de forma tempestiva, precisa e transparente. Ademais, sempre que o nível de risco ultrapassar o apetite ao risco da organização, o gestor deve comunicar imediatamente o Comitê de Gestão de Riscos, a fim de subsidiar a tomada de decisão em instância superior e garantir a efetividade da governança.

Cabe ainda ao gestor de riscos, nos casos em que o risco ultrapassar o apetite da organização e o respectivo plano de tratamento for aprovado pelo Comitê de Gestão de Riscos, comunicar regularmente a esse colegiado sobre a execução do referido plano. Esse procedimento assegura o acompanhamento sistemático das medidas implementadas, promove a transparência e reforça a responsabilidade compartilhada no processo de mitigação dos riscos.

Ressalta-se que a fidedignidade dos dados constitui elemento essencial diante da crescente utilização de sistemas informatizados de gestão e suporte à tomada de decisão. Nesse contexto, informações incorretas ou incompletas podem comprometer a identificação de riscos, resultar em análises imprecisas e, consequentemente, conduzir a decisões gerenciais equivocadas.

A avaliação da qualidade das informações requer a verificação de aspectos essenciais, tais como:

- a pertinência do conteúdo apresentado;
- a disponibilidade das informações em tempo hábil;
- a atualização dos dados utilizados;
- a exatidão e a confiabilidade das informações;
- a acessibilidade das informações às partes interessadas.

No que se refere à direção da comunicação, esta pode ser classificada em vertical e horizontal. A comunicação horizontal promove a difusão equitativa de informações entre unidades organizacionais distintas, assegurando alinhamento e cooperação nos processos transversais. Ademais, possibilita o assessoramento técnico especializado, favorecendo a correta aplicação da metodologia de gestão de riscos e continuidade do negócio, o adequado entendimento dos procedimentos e a identificação de situações que demandem deliberação em instâncias superiores.

Já a comunicação vertical ocorre tanto da base para a alta administração quanto em sentido inverso. Dessa forma, assegura-se que os gestores estejam informados sobre os riscos identificados em todas as unidades organizacionais e que os servidores conheçam os riscos mais relevantes que impactam a instituição.

A consulta, por sua vez, corresponde ao diálogo ativo e colaborativo com as partes interessadas, voltado à coleta de percepções, conhecimentos especializados e expectativas. Essa prática enriquece a base de informações disponível, fortalece a legitimidade das decisões e contribui para a construção de uma visão integrada dos riscos.

Convém que a comunicação e a consulta sejam planejadas e conduzidas de modo sistemático, contínuo e adaptado às especificidades da organização, utilizando canais apropriados e linguagem acessível, em conformidade com os princípios de ética, confidencialidade e transparência. Quando efetivamente implementadas, essas práticas fortalecem a governança, aprimoram a qualidade da tomada de decisões e ampliam a eficácia do processo de gestão de riscos.

Portanto, a etapa de comunicação e consulta deve ser compreendida não apenas como uma atividade de apoio, mas como um componente essencial e integrador da metodologia de gerenciamento de riscos, promovendo o alinhamento entre objetivos institucionais e interesses das partes envolvidas, além de contribuir para a resiliência e a sustentabilidade organizacional.

18 Monitoramento e Análise Crítica

A etapa de Monitoramento e Análise Crítica tem como propósito assegurar e aprimorar, de forma contínua, a qualidade e a eficácia da concepção, da implementação e dos resultados decorrentes do processo de gerenciamento de riscos. Trata-se de atividade estratégica que deve estar formalmente incorporada ao sistema de gestão da instituição, com responsabilidades claramente definidas e atribuídas aos atores envolvidos.

O monitoramento deve ser realizado de maneira contínua, enquanto a análise crítica deve ocorrer em intervalos planejados, abrangendo todos os estágios do processo de gerenciamento de riscos. Essa prática envolve o planejamento das atividades, a coleta e a análise sistemática de dados, o registro dos resultados e a disponibilização de informações consistentes que orientem a tomada de decisões e promovam a melhoria do desempenho institucional.

Compete aos gestores de riscos monitorar e realizar a análise crítica de seus respectivos riscos, de forma sistemática e baseada em evidências. Sempre que identificadas alterações significativas no cenário de riscos, tais como mudanças no ambiente interno ou externo, perda de eficácia das respostas adotadas ou redefinição de objetivos, os gestores devem reportar tempestivamente essas alterações à autoridade competente, assegurando a pronta resposta institucional e a atualização das medidas de controle.

O monitoramento ocorre de forma estruturada durante as Reuniões do Comitê Gestor de Riscos, instância responsável por acompanhar a evolução dos riscos e propor as ações corretivas cabíveis, analisar sugestões de atualização da Política de Gestão de Riscos e Continuidade do Negócio do Tribunal de Contas do Estado do Tocantins (TCETO), além de deliberar sobre ajustes e modificações de controle a serem incorporados ao Sistema de Gestão de Riscos da instituição.

A análise crítica do sistema de gestão de riscos é conduzida pela alta administração do TCETO, reunida no âmbito do Comitê Institucional de Governança, em intervalos previamente planejados, com a finalidade de assegurar a contínua adequação, suficiência, eficácia e alinhamento do processo de gestão de riscos ao direcionamento estratégico da instituição.

Nesse contexto, destacam-se as Reuniões de Análise da Estratégia, que integram o processo de monitoramento e nas quais são avaliadas a eficácia, a eficiência e a efetividade do Sistema de Gestão de Riscos. Essas análises têm por objetivo fortalecer a maturidade organizacional em governança e aprimorar a gestão de riscos.

19 Referências Bibliográficas

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000:2018: Gestão de riscos – Diretrizes. 2. ed. Rio de Janeiro, 2018.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 2030-1:2024 Ambiental, social e governança (ESG) Parte 1: Conceitos, diretrizes e modelo de avaliação e direcionamento para organizações. Rio de Janeiro, 2024.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 31073:2022: Gestão de Riscos – Vocabulário. 1. ed. Rio de Janeiro, 2022.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 31010:2021 – Gestão de Riscos – Técnicas para o processo de avaliação de riscos. 2. ed. Rio de Janeiro, 2021.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 31022:2020 – Gestão de Riscos – Diretrizes para a gestão de riscos legais. 1. ed. Rio de Janeiro, 2020.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 27005:2023 – Segurança da informação, segurança cibernética e proteção à privacidade - Orientações para gestão de riscos de segurança da informação. 4. ed. Rio de Janeiro, 2023.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 21504:2024 – Gerenciamento de projetos, programas e portfólio – Orientações sobre gestão de portfólio. 2. ed. Rio de Janeiro, 2024.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 21503:2024: Gerenciamento de projetos, programas e portfólios – Orientação sobre gestão de programas. 2. ed. Rio de Janeiro, 2024a.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 21502:2024: Gerenciamento de projetos, programas e portfólios – Orientação sobre gestão de projetos. 1. ed. Rio de Janeiro, 2024b.

20 Referências Bibliográficas

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 37000:2022: Governança de organizações - Orientações. 1. ed. Rio de Janeiro, 2022.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO ABNT 22301:2020: Segurança e resiliência - Sistema de gestão de continuidade de negócios - Requisitos. Rio de Janeiro, 2020.

- ASSOCIAÇÃO DOS MEMBROS DOS TRIBUNAIS DE CONTAS DO BRASIL (ATRICON). Resolução ATRICON nº 04, de 4 de dezembro de 2014 que aprova as diretrizes de controle externo relacionadas à temática controle interno: instrumento de eficiência dos Tribunais de Contas. Brasília, DF: ATRICON, 2014.