TRIBUNAL DE CONTAS
PERNAMBUCO

MANUAL DE GESTÃO DE RISCOS

DO TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO

Diretoria de Gestão e Governança - DGG

Recife, Julho 2026

MANUAL DE GESTÃO DE RISCOS DO TRIBUNAL DE CONTAS DO ESTADO DE PERNAMBUCO

A Gestão de Riscos no Tribunal de Contas do Estado de Pernambuco (TCE-PE) é um processo permanente, integrado à gestão e voltado a fornecer segurança razoável quanto ao alcance dos objetivos institucionais, por meio da identificação, análise, avaliação, tratamento e monitoramento dos riscos, com registro e relato sistemáticos. Essa atuação está ancorada na Política de Gestão de Riscos instituída pela Portaria Normativa nº 285, de 19 de agosto de 2025, que formaliza diretrizes e objetivos para fortalecer a gestão e ampliar a probabilidade de atingimento dos objetivos do TCE-PE.

Esta Metodologia será aplicada **a todos os processos e projetos** que dão suporte ao atingimento dos objetivos do TCE-PE.

A metodologia aqui apresentada adota como referência a **ABNT NBR ISO 31000:2018**, estruturando o processo de gestão de riscos em etapas interligadas e interativas, de modo a assegurar padronização, rastreabilidade e comparabilidade entre unidades e objetos analisados.

Adicionalmente, a metodologia está alinhada ao **Modelo das Três Linhas do IIA**, reforçando responsabilidades e salvaguardas: a **1ª linha** (gestores/proprietários do risco) executa a gestão de riscos no dia a dia; a **2ª linha (GAIN)** provê apoio metodológico, padronização e "challenge" para manter a exposição dentro do apetite/tolerância; e a **3ª linha**, também exercida pela GAIN, atua com **asseguração independente** sobre a adequação e efetividade da governança, gestão de riscos e controles, preservando sua independência ao não assumir responsabilidades gerenciais pelo processo.

A aplicação desta Metodologia é de responsabilidade primária do **gestor do processo (1ª linha)**, na qualidade de proprietário do risco, a quem compete assegurar a identificação, avaliação, tratamento e monitoramento dos riscos no âmbito do processo sob sua gestão, que receberá o apoio e orientação da 2ª linha, quando aplicável e também e mediante pedido da 1ª linha.

A revisão dos riscos deve ocorrer periodicamente e sempre que houver alterações relevantes no processo (mudanças normativas, reorganizações, implantação de sistemas, incidentes, achados de auditoria, ou outras situações que possam modificar a exposição a riscos, impactando a tolerância ou o apetite ao risco, mas sem alterar a metodologia em si).

1. REFERENCIAIS METODOLÓGICOS

A Metodologia de Gestão de Riscos do Tribunal de Contas do Estado de Pernambuco (TCE-PE) foi concebida com o objetivo de atender às exigências introduzidas pela Lei nº 14.133/2021, que reforçou a necessidade de adoção de práticas estruturadas de gestão de riscos e controles internos alinhadas a padrões reconhecidos nacional e internacionalmente.

O primeiro passo interno no TCE-PE foi a publicação da Portaria Normativa 285/2025, que estabeleceu as diretrizes da Política de Gestão de Riscos do órgão.

Nesse contexto, a utilização de referenciais metodológicos consolidados constitui elemento essencial para assegurar consistência conceitual, credibilidade técnica e aderência às melhores práticas de governança pública.

A adoção de frameworks e materiais de referência amplamente reconhecidos permite ao TCE-PE beneficiar-se de experiências acumuladas, modelos testados e lições aprendidas por organizações que já percorreram trajetórias de amadurecimento em gestão de riscos. Esses referenciais oferecem conceitos, princípios, estruturas de governança e instrumentos metodológicos que reduzem a subjetividade, promovem padronização mínima e favorecem a comparabilidade, sem prejuízo da necessária adaptação à realidade institucional do Tribunal.

Destacam-se, nesse sentido, os frameworks internacionais, como o **COSO – Enterprise Risk Management**, que contribui para a integração entre riscos, estratégia e desempenho organizacional; a **ABNT NBR ISO 31000:2018**, que estabelece princípios e diretrizes para a gestão de riscos de forma sistemática, estruturada e orientada à melhoria contínua; e as diretrizes do **The Institute of Internal Auditors (IIA)**, especialmente o modelo das Três Linhas, que orienta a adequada distribuição de responsabilidades e a preservação da independência das funções de controle.

Paralelamente, a metodologia incorpora aprendizados oriundos de experiências nacionais relevantes, notadamente de órgãos de controle e instituições públicas que enfrentam desafios semelhantes aos do TCE-PE. As publicações e manuais da **Controladoria-Geral da União (CGU)** e do **Tribunal de Contas da União (TCU)** oferecem referenciais importantes sobre governança, gestão de riscos e avaliação de maturidade, permitindo ao Tribunal alinhar-se às práticas exigidas dos jurisdicionados e fortalecer a coerência entre o controle externo exercido e a gestão interna adotada.

Do mesmo modo, a análise de metodologias desenvolvidas por outros tribunais, como o **Tribunal de Justiça de Goiás (TJ-GO), Tribunal de Justiça do Distrito Federal (TJ-DF)** e o **Tribunal de Contas do Ceará (TCE-CE)**, bem como de organismos internacionais de auditoria governamental, a exemplo do **National Audit Office (NAO)**, possibilitou identificar soluções práticas, níveis adequados de detalhamento e estratégias de implementação compatíveis com o setor público.

A utilização desses materiais de referência não implica adoção automática ou reprodução integral de modelos externos, mas sim a seleção crítica de conceitos, práticas e instrumentos que contribuam para o fortalecimento da governança, o desenvolvimento da cultura de riscos e o amadurecimento progressivo do Processo de Gestão de Riscos do TCE-PE, respeitadas suas especificidades institucionais, normativas e organizacionais.

2. COMPETÊNCIAS NA GESTÃO DE RISCOS

Conforme definido pela Portaria Normativa n° 285/2025, **a gestão de riscos no âmbito do Tribunal de Contas do Estado de Pernambuco** (TCE/PE) constitui responsabilidade compartilhada, devendo ser exercida de forma integrada aos objetivos estratégicos, em conformidade com o modelo das **Três Linhas**, conforme proposto pelo *The Institute of Internal Auditors (IIA)*. Nesse modelo:

- **Primeira Linha**: é integrada pelas unidades organizacionais, pelos proprietários de riscos e pelos servidores envolvidos na execução das atividades do TCE/PE, responsáveis pela gestão direta e cotidiana dos riscos e pela implementação e manutenção dos controles internos nos processos sob sua responsabilidade;
- **Segunda Linha**: responsável por estabelecer diretrizes, metodologias e orientações, bem como por supervisionar e monitorar, em nível institucional, a gestão de riscos e os controles internos executados pela Primeira Linha.

A GAIN é a unidade central responsável pela coordenação metodológica e institucional da gestão de riscos e do sistema de integridade;

Outras unidades, como PROJUR e CORR, podem atuar como instâncias de apoio especializado em seus temas próprios, **sem assumir a centralidade metodológica da gestão de riscos**.

- **Terceira Linha**: é exercida também pela Gerência de Auditoria Interna (GAIN), que atua de forma independente e objetiva, avaliando a adequação e a efetividade da gestão de riscos e dos controles internos, e emitindo recomendações para o seu aprimoramento, sem assumir responsabilidades de gestão ou execução.

A atuação das instâncias e dos papéis definidos nesta Metodologia deve observar, obrigatoriamente, **o princípio da segregação de funções**, de modo a preservar a objetividade, a independência e a eficácia da Gestão de Riscos no TCE/PE.

Excepcionalmente, em caráter transitório, enquanto não houver estrutura específica para assegurar a separação plena entre a 2ª e a 3ª linhas, a GAIN exercerá cumulativamente as funções de coordenação da gestão de riscos, coordenação do sistema de integridade e auditoria interna, devendo ser adotadas salvaguardas procedimentais para mitigação de conflitos entre as atividades de orientação, coordenação, monitoramento e avaliação independente.

Para fins desta Metodologia, são definidos os seguintes papéis essenciais:

1. Conselho de Governança Institucional (CGI)

Como instância estratégia da gestão de riscos no TCE/PE, compete ao Conselho de Governança Institucional:

- estabelecer o direcionamento estratégico da gestão de riscos;
- definir e revisar o apetite a risco institucional;
- aprovar a Metodologia de Gestão de Riscos do TCE/PE e suas atualizações;
- estabelecer diretrizes, objetivos e indicadores relativos à Gestão de Riscos;

- deliberar, quando necessário, sobre riscos estratégicos que extrapolem o nível tático;
- promover o alinhamento entre a gestão de riscos, o planejamento estratégico e a governança institucional.
- supervisionar a atuação das demais instâncias da Gestão de Riscos;
- assegurar o apoio institucional necessário à implementação e ao funcionamento da Gestão de Riscos;
- promover e fortalecer a cultura organizacional de gestão de riscos.

2. Conselho de Gestão de Riscos (CGR)

Como instância tática da gestão de riscos no TCE/PE, compete ao Conselho de Gestão de Riscos (CGR):

- auxiliar o CGI na execução de suas competências;
- coordenar, em nível institucional, a aplicação da Metodologia de Gestão de Riscos;
- avaliar a Metodologia de Gestão de Riscos e suas atualizações;
- consolidar informações sobre riscos relevantes provenientes das unidades organizacionais;
- monitorar a evolução dos níveis de risco e o desempenho das medidas de tratamento empregadas;
- elaborar relatórios gerenciais de monitoramento e avaliação
- propor diretrizes, prioridades e orientações para o tratamento de riscos;
- definir os requisitos funcionais necessários para o acesso às ferramentas de suporte ao processo de gerenciamento de riscos;

3. Subcomissão Temática da Gestão de Riscos (STGR)

Como instância de apoio operacional à Gestão de Riscos, compete à Subcomissão Temática de Gestão de Riscos (STGR):

- apoiar o CGI e o CGR no monitoramento da gestão de riscos no nível operacional;
- acompanhar a aplicação da Metodologia de Gestão de Riscos nas unidades organizacionais;
- auxiliar na consolidação de informações operacionais sobre riscos, controles e ações de tratamento;
- promover a articulação entre as unidades organizacionais no tratamento de riscos transversais;
- contribuir para a disseminação da cultura de gestão de riscos no TCE/PE;
- executar outras atividades correlatas definidas pelo CGR ou pelo CGI.

4. Proprietários de Riscos (Primeira Linha)

Os Proprietários de Riscos são os gestores responsáveis, ou formalmente designados, pelos processos, atividades, projetos ou unidades organizacionais. Integram a **Primeira Linha**,

sendo os responsáveis pela gestão de riscos direta e cotidiana dos riscos sob sua responsabilidade. Compete a eles:

- identificar, analisar e avaliar os riscos sob sua responsabilidade;
- implementar e manter controles e ações de tratamento de riscos;
- monitorar a evolução dos riscos e a eficácia das respostas adotadas;
- comunicar tempestivamente riscos relevantes às instâncias superiores;
- manter registros atualizados dos riscos e das ações de tratamento.

5. Unidades Organizacionais (Primeira Linha)

As unidades organizacionais do TCE/PE, no exercício de suas atividades, integram a **Primeira Linha** e são responsáveis por:

- aplicar a Metodologia de Gestão de Riscos nos processos sob sua competência;
- colaborar com as instâncias de governança e apoio metodológico;
- incorporar a análise de riscos à gestão cotidiana e à tomada de decisão.

6. Servidores (Primeira Linha)

Todos os servidores do TCE-PE são responsáveis por identificar e comunicar os riscos em suas atividades diárias.

7. Gerência de Auditoria Interna – GAIN

A Gerência de Auditoria Interna (GAIN), como instância de apoio metodológico e supervisão técnica, atua como **Segunda Linha**, competindo-lhe:

- definir, manter e atualizar a Metodologia de Gestão de Riscos do TCE/PE, observados os direcionamentos do CGI;
- orientar tecnicamente as unidades organizacionais quanto à aplicação da metodologia;
- promover a integração da gestão de riscos com a gestão de processos;
- consolidar informações institucionais sobre riscos e apoiar o monitoramento sistêmico;
- fomentar a capacitação e a disseminação da cultura de gestão de riscos no Tribunal.

Além disso, a Gerência de Auditoria Interna (GAIN), atuando como **Terceira Linha**, de forma independente e objetiva, competindo-lhe:

- avaliar a adequação e a efetividade do Processo de Gestão de Riscos do TCE/PE;
- verificar a conformidade da aplicação da metodologia com os normativos institucionais;
- emitir recomendações para o aprimoramento da gestão de riscos;
- resguardar sua independência, não assumindo responsabilidades de gestão ou de execução de riscos.

3. INTEGRAÇÃO DA GESTÃO DE RISCOS AOS PROCESSOS ORGANIZACIONAIS

Como parte do Planejamento Estratégico 2026–2031, é fundamental que a gestão de riscos no âmbito do Tribunal de Contas do Estado de Pernambuco (TCE-PE) esteja integrada aos processos organizacionais, de modo a subsidiar a tomada de decisão, o alcance dos objetivos estratégicos e o fortalecimento da governança institucional. Essa integração constitui diretriz e princípio da Gestão de Riscos, conforme disposto na Portaria Normativa nº 285/2025 do TCE-PE.

Nesse contexto, a integração da gestão de riscos aos processos organizacionais configura-se como princípio estruturante desta Metodologia, devendo ocorrer de forma contínua e sistemática, e ser compatível com a natureza, a complexidade e a criticidade dos processos envolvidos, de modo a assegurar que riscos e oportunidades sejam considerados de maneira proporcional e tempestiva ao longo do ciclo de planejamento, execução, monitoramento e revisão das atividades institucionais.

Considerando a diversidade de processos existentes no âmbito do TCE-PE, em razão de suas atribuições envolvidas no exercício do controle externo, não se pode adotar um modelo único e rígido de integração, de modo a preservar a efetividade, a proporcionalidade e a aderência às boas práticas de gestão de riscos.

Nesse sentido, a Metodologia estabelece os conceitos, princípios, papéis e etapas do processo de gestão de riscos, cabendo às gerências, com apoio da Gerência de Auditoria Interna (GAIN), que atuará como Segunda Linha, integrar a análise de riscos aos seus processos de trabalho, observadas as diretrizes institucionais e as características específicas de cada processo.

A integração da gestão de riscos aos processos organizacionais deverá ocorrer, no mínimo, nas seguintes situações:

I – no planejamento e na revisão de processos, atividades ou projetos relevantes;

II – na definição de objetivos estratégicos, táticos ou operacionais;

III – na ocorrência de mudanças significativas no ambiente interno ou externo;

IV – na identificação de riscos relevantes ou críticos que possam comprometer o alcance dos objetivos estratégicos.

A Gerência de Auditoria Interna (GAIN), como Segunda Linha, prestará apoio metodológico às demais gerências, promovendo a harmonização das práticas de integração, sem prejuízo da responsabilidade da Primeira Linha pela gestão direta dos riscos associados aos seus processos.

Assim, o gerenciamento de riscos irá acontecer de forma simultânea ao gerenciamento de processos.

3.1. CAPACITAÇÃO

O diagnóstico de maturidade da gestão de riscos, realizado no âmbito do Tribunal de Contas do Estado de Pernambuco (TCE-PE) por meio do Relatório de Consultoria n° 02 da GAIN, evidenciou que o desenvolvimento e a consolidação da cultura de gestão de riscos

dependem, de forma decisiva, da capacitação contínua dos gestores e servidores envolvidos nos processos institucionais. Nesse contexto, a capacitação constitui elemento estruturante desta Metodologia e condição essencial para sua adequada implementação e evolução.

A gestão de riscos requer conhecimentos técnicos, habilidades analíticas e compreensão conceitual que não se esgotam na edição de normativos ou na definição de procedimentos formais, sendo necessário promover o aprendizado progressivo e permanente sobre conceitos, ferramentas, responsabilidades e boas práticas relacionadas à identificação, avaliação, tratamento, monitoramento e comunicação de riscos.

A capacitação deverá ser tratada como processo contínuo e evolutivo, alinhado aos ciclos de melhoria da gestão de riscos, de modo a acompanhar mudanças no ambiente institucional, no perfil dos riscos e no grau de complexidade dos processos do Tribunal, contribuindo para a efetividade, a sustentabilidade e o amadurecimento do Processo de Gestão de Riscos.

A capacitação contínua em gestão de riscos tem por finalidade assegurar a aplicação consistente da Metodologia, reduzir assimetrias de entendimento entre as gerências, fortalecer a atuação da Primeira Linha e aprimorar a qualidade das informações fornecidas às instâncias de governança.

Como estabelecido pelo Art. 10 da Portaria Normativa 285/2025 do TCE-PE, o Conselho de Governança Institucional (CGI) é responsável por promover a cultura de gestão de riscos no órgão.

A Diretoria de Gestão e Governança (DGG) promoverá treinamentos regulares sobre Gestão de Riscos, com vistas a promover a cultura de gestão de riscos no TCE-PE e disseminar as boas práticas nessa área, observados os direcionamentos do Conselho de Governança Institucional (CGI).

4. A DEFINIÇÃO DO APETITE AO RISCO

A definição do apetite ao risco constitui elemento essencial para a efetividade da gestão de riscos no Tribunal de Contas do Estado de Pernambuco (TCE-PE). De acordo com o Principle Two e o Principle Three do gerenciamento de riscos do National Audit Office (NAO), a gestão de riscos é mais eficaz quando os níveis de risco que a organização está disposta a aceitar no cumprimento de seus objetivos estratégicos são definidos de maneira clara e explícita.

*Enquanto o apetite ao risco orienta a tomada de decisão estratégica, a tolerância a risco auxilia na priorização de controles e no adequado escalonamento de riscos às instâncias de governança.*Também orienta a atuação da Primeira e da Segunda Linhas, conferindo maior clareza quanto aos níveis de exposição aceitáveis, aos critérios de tratamento de riscos e às situações que demandam escalonamento às instâncias superiores de governança.

No âmbito do TCE-PE, compete ao Conselho de Governança Institucional (CGI) estabelecer o apetite ao risco institucional e as diretrizes para a fixação da tolerância a riscos em processos, projetos ou áreas estratégicas, observadas as diretrizes da Política de Gestão de Riscos.

Também é papel do CGI revisar o apetite ao risco periodicamente, considerando mudanças no ambiente interno e externo, no planejamento estratégico e no perfil de riscos do Tribunal, de forma a manter sua aderência às condições institucionais e ao interesse público.

O Comitê de Gestão de Riscos (CGR) apoiará o CGI na proposição, revisão e desdobramento do apetite ao risco, promovendo sua comunicação às gerências e sua incorporação aos processos de gestão, de modo a assegurar decisões mais consistentes, proporcionais e alinhadas às prioridades institucionais.

5. O PROCESSO DE GESTÃO DE RISCOS

Conforme definido pela Portaria Normativa n° 285 do TCE-PE, o processo de gestão de riscos compreende as seguintes etapas:

1. **Estabelecimento do Contexto**
2. **Identificação de Riscos**
3. **Avaliação de Riscos** (Análise e Avaliação):
    a. **Avaliação do Risco**
    b. **Avaliação do controle**
4. **Respostas aos Riscos**
5. **Monitoramento** (Transversal)
6. **Comunicação** (Transversal)

5.1. ESTABELECIMENTO DO CONTEXTO (pré avaliação e análise do ambiente)

Esta etapa consiste em compreender e caracterizar **o ambiente externo e interno** no qual o objeto de gestão de riscos (**processo, projeto, meta ou unidade)** se encontra inserido, delimitando fronteiras, objetivos, partes interessadas e critérios que orientarão a identificação, análise e avaliação dos riscos.

Não basta apenas analisar o ambiente; é necessário definir parâmetros (premissas, horizonte temporal, critérios e dimensões de impacto) e critérios. O objetivo é compreender as variáveis que podem alterar esse ambiente e definir onde a gestão será aplicada.

A fim de estabelecer corretamente o contexto do objeto, devem ser reunidos, conforme aplicável:

- documentos normativos e regulatórios pertinentes (internos e externos);
- descrição do processo/atividade (fluxos, procedimentos, sistemas utilizados, interfaces);
- metas, indicadores e objetivos associados ao objeto;
- registros de ocorrências, falhas, incidentes, achados de auditoria, reclamações e lições aprendidas;
- organograma, papéis e responsabilidades envolvidos no objeto;
- contratos relevantes, fornecedores críticos e dependências externas.

5.1.1. Passos Essenciais

1. Definir o Objeto: descrever claramente o que será analisado (Ex: Processo de Contratação, Meta de Auditoria, Segurança da Informação), incluindo:

- as fronteiras do objeto, isto é, o início e o fim;
- suas principais entregas;
- interfaces com outras unidades e sistemas;
- suas dependências críticas, como, em relação a pessoas-chave, tecnologias, fornecedores, informações e prazos.

2. Identificar Objetivos: registrar os resultados a serem alcançados pelo objeto, e, sempre que possível, vinculá-los a indicadores de desempenho. Adicionalmente, explicitar critérios caracterizando o que seria o sucesso e o que seria a falha no cumprimento dos objetivos.

3. Mapear Partes Interessadas (*Stakeholders*): identificar quem são as pessoas ou setores (internos e externos) que influenciam ou são influenciados pelo objeto. Para cada grupo relevante, registrar:

- sua expectativa ou necessidade em relação ao objeto;
- seu grau de influência (alto, médio ou baixo) em relação aos resultados;
- impacto do não atingimento dos objetivos sobre eles.

4. Análise SWOT: é uma ferramenta de diagnóstico usada para **mapear fatores internos e externos** que podem influenciar o alcance dos objetivos do objeto analisado. Ela organiza o contexto, ajudando a tornar a etapa de riscos mais consistente e completa. por meio dessa ferramenta pode-se:

- identificar condicionantes do ambiente que favorecem ou dificultam o alcance dos objetivos;
- revelar vulnerabilidades e capacidades que podem se relacionar a riscos;
- apoiar a seleção de riscos relevantes e a definição de critérios e premissas.

A SWOT separa os fatores envolvidos em dois eixos:

Fatores Internos, que são aqueles controláveis, ao menos, parcialmente pelo TCE-PE:

- **Forças (Strenghts):** recursos, capacidades, controles existentes, competëncias, sistemas, estrutura e práticas que favorecem o desempenho;
- **Fraquezas (Weaknesses):** limitações internas, gargalos, insuficiência de recursos, falhas de processo, lacunas de competências, dependências críticas e controles frágeis.

Fatores Externos, que são aqueles fora do controle direto do TCE-PE:

- **Oportunidades (Opportunities):** tendências, mudanças e condições externas que podem ser aproveitadas para melhorar resultados, como novas tecnologias, cooperação, padronização e mudanças regulatórias favoráveis;
- **Ameaças (Threats):** condições externas que podem comprometer objetivos, como mudanças legais, restrições orçamentárias, riscos reputacionais, eventos externos e indisponibilidade de fornecedores.

Ferramenta: Matriz SWOT (Análise de Ambiente) Conforme as melhores práticas adotadas, utiliza-se a Matriz SWOT para mapear o cenário antes de identificar os riscos,de acordo com o quadro explicativo abaixo (Quadro 1 - Matriz SWOT):

Quadro 1 - Matriz SWOT

FATORES INTERNOS	**FATORES EXTERNOS**
FORÇAS (*Strengths*) (Positivo)	**OPORTUNIDADES (*Opportunities*)** (Positivo)
Características internas que favorecem o desempenho e o atingimento da missão do TCE-PE.	Características externas (ambiente legal, social, político) que podem ajudar a melhorar o desempenho.
FRAQUEZAS (*Weaknesses*) (Negativo)	**AMEAÇAS (*Threats*)** (Negativo)
Deficiências internas, falta de recursos ou falhas em processos que inibem o desempenho.	Fatores externos não controláveis que podem comprometer os objetivos estratégicos.

Para que a Matriz SWOT seja útil e registrável no manual, cada item deve ser:

- específico e verificável;
- relacionado a um objetivo do objeto, sendo importante mostrar a ligação com o que precisa ser entregue;

- redigido como fator, não como risco, pois a SWOT descreve o contexto;
- não duplicado entre quadrantes;
- sempre que possível, com evidência ou referência.

5.1.2. Papéis e Responsabilidades

Conforme definido na Política de Gestão de Riscos (Portaria Normativa nº 285/2025), a condução desta etapa de Estabelecimento de Contexto é de competência exclusiva do Gestor do Processo (1ª linha). O apoio metodológico da GAIN (2ª linha) deve ser solicitado pelo gestor sempre que houver necessidade de padronização, orientação técnica ou questionamento de premissas. Para a execução desta etapa, recomenda-se que o gestor articule a participação de representantes das áreas que executam atividades-chave, unidades provedoras e partes interessadas relevantes, garantindo uma visão sistêmica do objeto.

5.2. IDENTIFICAÇÃO DE RISCOS

Nesta etapa, identificam-se os eventos incertos que podem afetar a realização dos objetivos do objeto analisado, determinando suas causas e consequências.

O propósito é encontrar, reconhecer e descrever os eventos de riscos, causas e consequências de forma consistente e rastreável, fornecendo base para as etapas de análise, avaliação e tratamento.

5.2.1 Como Identificar os Riscos

Para uma identificação eficaz, o gestor deve responder à pergunta-chave:

"O que pode atrapalhar ou impedir o alcance do objetivo/resultado?"

Para ampliar a qualidade da discussão, é importante se questionar:

- O que pode dar errado? (falhas operacionais, humanas, sistêmicas)
- O que pode mudar no ambiente? (normas, demandas externas, orçamento, tecnologia)
- Já tivemos problemas? (verificar o histórico de falhas, ocorrências e lições aprendidas)

Quais dependências críticas (tecnologias, fornecedores, insumos ou pessoas-chave) são essenciais para o processo e quão vulneráveis elas estão a falhas ou interrupções?

5.2.2 Técnicas Sugeridas

- **Brainstoming:** é um reunião em que um grupo de participantes compartilha livremente suas ideias sobre riscos em um tempo definido, é muito útil para ampliar hipóteses rapidamente;
- **Brainwriting (escrita cerebral):** cada participante registra riscos anonimamente e em silêncio antes de debater, reduzindo o viés de autoridade e aumentando a coleta de ideias.
- **Diagrama Bow Tie:** ferramenta visual para aprofundar um risco específico, estruturando causas, barreiras preventivas, evento, consequências e barreiras mitigadoras.

Atenção: Deve-se distinguir o risco (evento futuro e incerto) do problema (fato já concretizado). Se o evento já ocorreu, ele deve ser tratado como problema, não como risco.

5.2.3. Técnica de Descrição do Risco (Sintaxe Padrão)

Para garantir a clareza, o TCE-PE adota a seguinte estrutura de redação para o registro dos riscos, baseada na relação de causa e efeito:

> **"Devido a [CAUSA/FONTE], poderá acontecer [EVENTO/RISCO], o que poderá levar a [CONSEQUÊNCIA/IMPACTO] impactando no objetivo."**

5.2.4. Ferramenta Visual: Diagrama Bow Tie (Gravata Borboleta)

Quanto à ferramenta visual denominada **"Diagrama *Bow Tie"* (Gravata Borboleta)**, para análise aprofundada das causas e consequências, utiliza-se o modelo esquemático do quadro abaixo:

Quadro 2 - Modelo Esquemático: Análise das Causas e Consequências

CAUSAS (Fontes)	**EVENTO (Risco) [NOME DO RISCO]**	**CONSEQUÊNCIAS (Impactos)**
1. Falha em sistema... 2. Equipe reduzida... 3. Ausência de norma…	$\leftarrow$	1. Atraso processual... 2. Dano à imagem... 3. Prejuízo financeiro…
CONTROLES PREVENTIVOS *(Atuam sobre a causa)*	**CENTRO** $\rightarrow$	**CONTROLES MITIGADORES** *(Atuam sobre a consequência)*

No diagrama Bow Tie:

- **EVENTO/RISCO** deve ser formulado como algo que pode ocorrer (ex.: atraso na tramitação, pagamento indevido, Falha no acesso ao sistema, etc.);
- **CAUSA/FONTE** deve explicar por que pode ocorrer;

- **CONSEQUÊNCIA/IMPACTO** deve apontar o impacto potencial do risco sobre os objetivos do objeto.

É importante esclarecer que os riscos devem ser analisados de forma pura, isto é, isolados dos controles empregados nas atividades diárias. Os controles podem ser de dois tipos:

- **Controles Preventivos:** atuam sobre a causa, visando a diminuir as chances de materialização do risco;
- **Controles Mitigadores:** atuam sobre as consequência, visando a diminuir os danos que o risco pode ocasionar aos objetivos do TCE-PE.

Ao final da identificação, deve existir:

- **Lista consolidada de riscos** do objeto contendo o objetivo relacionado, a descrição do risco, causas/fontes, consequências/impactos e controles existentes, quando aplicável;
- **Diagrama Bow Tie** para riscos priorizados.

5.3. AVALIAÇÃO DE RISCOS (ANÁLISE E AVALIAÇÃO)

Esta etapa envolve a análise (compreensão da natureza do risco) e a avaliação (comparação com critérios de aceitação).

5.3.1. Análise

A análise combina a probabilidade e o impacto para determinar o nível de risco, além de avaliar os controles existentes.

• **Importante:** A análise deve considerar diferenciar **o risco inerente,** que é o nível de risco antes de considerar qualquer controle existente, **do risco residual**, ou seja, com os controles que já existem e estão em funcionamento (Risco Real/Residual).

• **Prevalência do Impacto:** o impacto é a dimensão mais importante. Um evento de impacto "Muito Alto" e probabilidade "Rara" deve preocupar o gestor mais do que um evento de probabilidade "Alta" e impacto "Baixo" (se o impacto é mínimo, o risco é tolerável).

5.3.2. Avaliação

O nível de risco encontrado é comparado com a **Tolerância a Riscos** definida para o objeto analisado (processo, projeto ou atividade). A tolerância representa os limites de variação aceitável para o atingimento dos objetivos específicos deste objeto, os quais devem estar alinhados ao **Apetite ao Risco** institucional estabelecido pelo Conselho de Governança Institucional (CGI).

• **Faixa Vermelha (Acima do limite):** O risco é inaceitável e *deve* ser tratado.

• **Faixa Amarela (Alerta):** Deve ser avaliada a necessidade de monitoramento contínuo.

• **Faixa Verde (Abaixo do limite):** O risco é aceitável, não exigindo ações imediatas além dos controles já existentes

Esta etapa envolve a análise da probabilidade e do impacto dos riscos, observados os controles existentes.

5.3.3. Escalas de Mensuração

Segundo o padrão metodológico, classificam-se os riscos em:

- **Probabilidade (P):** 1. Raro | 2. Pouco Provável | 3. Provável | 4. Muito Provável | 5. Praticamente Certo.
- **Impacto (I):** 1. Muito Baixo | 2. Baixo | 3. Médio | 4. Alto | 5. Muito Alto.

Os riscos potenciais terão seu impacto avaliado de acordo com a escala de impactos que vai desde o risco muito baixo ao muito alto[1].

Escala de Impactos		
Magnitude	**Descrição**	
Muito baixo	Impacto irrisório nos resultados; não afeta cronograma ou qualidade; sem prejuízo financeiro ou reputacional.	1
Baixo	Impacto pequeno nos resultados; pequenos atrasos ou custos adicionais absorvíveis sem impacto nas metas.	2
Médio	Impacto relevante nos resultados; atraso no cronograma ou perda de qualidade que exige ajustes no plano de ação.	5
Alto	Impacto grave; não atingimento de metas parciais; necessidade de intervenção para evitar comprometimento do objetivo.	8
Muito alto	Impacto catastrófico; impossibilidade de atingir o objetivo principal; danos irreversíveis à imagem ou prejuízo financeiro grave.	10

A seguinte tabela será utilizada escala de probabilidades para classificar as probabilidades de ocorrência dos riscos mapeados.

Escala de Probabilidades		
Magnitude	**Descrição**	
Muito baixo	Evento remotamente possível; histórico inexistente ou altamente improvável no cenário atual.	1

[1] inspirada em Fonte: Brasil. Tribunal de Contas da União. Roteiro de Auditoria de Gestão de Riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017.

Escala de Probabilidades		
Magnitude	**Descrição**	
Baixo	Evento pouco frequente; existem precedentes, mas são incidentes isolados.	2
Médio	Evento possível; ocorre periodicamente ou há indícios de que pode ocorrer.	5
Alto	Evento frequente; é esperado que ocorra regularmente dado o cenário atual.	8
Muito alto	Evento quase certo; praticamente inerente às atividades atuais; ocorre com alta frequência.	10

Exemplo de aplicação

Exemplo: Em um processo de aquisição de bens, o risco de "atraso na entrega pelo fornecedor" pode ser avaliado como **Impacto Médio (5)**, pois afeta o cronograma, mas não o objetivo final de entrega, e **Probabilidade Média (5)**, considerando o histórico recente de dificuldades logísticas do mercado.

5.3.4. Matriz de Riscos (Mapa de Calor)

A combinação de Probabilidade e Impacto define o Nível de Risco Inerente ou Residual. A matriz abaixo orienta a priorização:

IMPACTO PROBABILIDADE	**Raro**	**Pouco Provável**	**Provável**	**Muito Provável**	**Praticamente Certo**
Muito Alto	Médio (10)	Alto (20)	Alto (50)	Extremo (80)	Extremo (100)
Alto	Médio (8)	Médio (16)	Alto (40)	Alto (64)	Extremo (80)
Médio	Baixo (5)	Médio (10)	Médio (25)	Alto (40)	Alto (50)
Baixo	Baixo (2)	Médio (4)	Médio (10)	Médio (16)	Médio (20)
Muito Baixo	Baixo (1)	Baixo (2)	Baixo (5)	Médio (8)	Médio (10)

A matriz de riscos facilita o cálculo do risco inerente, que consiste no produto da probabilidade (P) pelo impacto (I).

Risco Inerente (RI) = Impacto (I) x Probabilidade (P)

Seguindo o exemplo anterior, o risco inerente calculado para o atraso na entrega pelo fornecedor seria enquadrado como médio (5 x 5 = 25).

Deve-se destacar que **o impacto é a dimensão mais importante dessa matriz**, de modo que um evento de impacto muito alto e probabilidade muito baixa merece mais atenção do que um evento de impacto muito baixo e probabilidade muito alta.

O risco inerente é o nível de risco antes de considerar qualquer controle existente – isto é, sem qualquer conferência, checagem, sistemas, revisões etc.

O nível de risco inerente não pode ser extraído diretamente da frequência com que ele se materializa nas atividades diárias do órgão, pois essa frequência é contaminada pela atuação dos controles existentes.

Por exemplo, o risco inerente de pagar por um serviço não realizado é alto. Um erro comum é imaginar que esse risco é baixo, porque são feitas fiscalizações e conferências. Porém, essas fiscalizações e conferências são atividades de controle, que serão avaliadas mais adiante.

No risco de **contratação com sobrepreço**, o gestor avalia que "o risco é baixo porque fazemos pesquisa de preços e a área técnica revisa o termo de referência". Na realidade, isso significa reconhecer que o risco inerente de sobrepreço pode ser relevante, mas que os controles (pesquisa de preços, revisão técnica, parecer, validações) reduzem a exposição após sua aplicação.

Ao classificar o **risco inerente**, o gestor deve avaliar a exposição **bruta**, como se **não existisse nenhum controle**. Sempre que o raciocínio começar com "o risco é baixo **porque**…", é um sinal de que o "porque" está descrevendo um **controle existente**. Nesse caso, o risco inerente pode ser alto, mas o controle reduz a exposição e, portanto, pode reduzir o **risco residual**. Será mostrado um exemplo dessa situação na seção 5.4.1.

5.3.5. Legenda de Níveis de Risco e Critérios de Aceitabilidade

A seguir, apresenta-se a legenda de níveis de risco adotada nesta Metodologia, obtida a partir do risco inerente resultante da combinação entre Probabilidade e Impacto na matriz corporativa.

Essa classificação padroniza a leitura dos riscos e permite verificar se o nível de risco encontrado está dentro da **tolerância** definida para o processo. A matriz avalia a

aceitabilidade do risco, indicando se ele exige novas ações de controle ou se está dentro dos parâmetros de tolerância estabelecidos.

- **EXTREMO (80–100)** – **Inaceitável**. Tratamento **obrigatório e imediato**. Elaborar Plano de Tratamento em até **15 dias úteis** e submeter para ciência/decisão do **CGR/CGI**.

- **ALTO (40–79)** – **Inaceitável**. Tratamento **obrigatório**. Elaborar Plano de Tratamento em até **60 dias úteis** e acompanhar até redução para Médio ou Baixo.

- **MÉDIO (8–39)** – **Tolerável sob controle**. Definir ação de melhoria *ou* aceitação formal com justificativa, mantendo monitoramento trimestral ou semestral.

- **BAIXO (1–7)** – **Aceitável**. Manter controles existentes e revisar no ciclo regular de monitoramento anual.

5.4. RESPOSTAS AOS RISCOS (TRATAMENTO)

A decisão de tratar deve considerar a viabilidade técnica, os recursos disponíveis, a conformidade legal e a relação custo-benefício (o custo do controle deve ser proporcional ao nível do risco e aos benefícios esperados para o alcance dos objetivos).
Tipos de Medidas (Modelo Bow-Tie/TCU): Ao definir o tratamento, o gestor deve atacar as causas ou as consequências:

1. **Medidas Preventivas (Causas):** Atuam nos gatilhos para reduzir a **Probabilidade** (Ex: Segregação de funções, capacitação).
2. **Medidas Detectivas (Controle):** Identificam a falha ou desvio assim que ocorrem (Ex: Auditorias, revisões, alertas automáticos).
3. **Medidas Corretivas (Correção):** Reparar o erro ou falha após a identificação (Ex: Ajuste de registros, reprocesso).
4. **Medidas de Contingência (Consequências):** Atuam para reduzir o **Impacto** caso o risco se concretize (Ex: Backups, planos de recuperação, seguros).

Nesta etapa, definem-se as ações para adequar os riscos ao **Apetite a Risco** do TCE-PE (quantidade de risco que o Tribunal aceita para exercer suas atividades).

As opções de tratamento são:

1. **Evitar:** consiste em eliminar a exposição, descontinuando a atividade que gera o risco ou redesenhando o processo para remover a causa. É usada quando se trata de uma atividade não-essencial, o risco está acima do apetite e não há mitigação viável.
2. **Mitigar:** reduzir a probabilidade ou o impacto por meio de **novos controles ou fortalecimento** dos já existentes. Pode incluir controles preventivos (evitam), detectivos (identificam), corretivos (corrigem) e de contingência (reduzem impacto).

A mitigação é usada quando a atividade é necessária, mas o nível de risco precisa cair para dentro da tolerância do TCE-PE.

3. **Compartilhar:** transferir parte do risco para terceiros (ex: seguros, terceirização, cláusulas contratuais e garantias). O compartilhamento não transfere totalmente o risco de **responsabilidade institucional**. Esse tratamento deve ser utilizado quando terceiros conseguem gerir melhor parte do risco.
4. **Aceitar:** manter o risco no nível atual (se estiver dentro da tolerância), sem adotar medidas adicionais. A aceitação é usada quando o risco é baixo ou o custo de tratar é maior que o benefício, não havendo ações de tratamento razoáveis. Mesmo assim, a decisão de aceitação deve ser registrada e justificada, e, sempre que possível, o risco deve ser monitorado.

5.4.1. Atividades de Controle

Conhecidos os principais riscos inerentes, deve-se proceder a uma avaliação a respeito dos mecanismos de controle adotados a fim de mitigá-los.

A escala de avaliação preliminar dos controles adotados é mostrada a seguir.

Escala de avaliação preliminar dos Controles (desenho e implementação)

Avaliação do Controle*	Situação do controle existente	Nível de Confiança nos controles (NC)	Risco de Controle (RC), ou seja, 1 - NC
Inexistente	Controle não existe, não funciona ou não está implementado.	**Nenhum nível de confiança. Considerando RI igual a 1,00 e NC igual a zero, temos 1,00 - 0.**	1,00
Fraco	Controle não institucionalizado; está na esfera de conhecimento pessoal dos operadores do processo; em geral realizado de maneira manual.	**Nível de Confiança de 20%.** Os controles são capazes de mitigar 20% dos eventos. Risco de controle = 1,00 - 0,20.	0,80
Mediano	Controle razoavelmente institucionalizado, mas pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	**Nível de Confiança de 40%.** Os controles são capazes de mitigar 40% dos eventos. Risco de controle = 1,00 - 0,40.	0,60
Satisfatório	Controle institucionalizado e embora passível de aperfeiçoamento, é sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	**Nível de Confiança de 60%.** Os controles são capazes de mitigar 60% dos eventos. Risco de controle = 1,00 - 0,60.	0,40
Forte	Controle institucionalizado e sustentado por ferramentas adequadas, podendo ser considerado em um nível de "melhor prática"; mitiga o risco em todos os aspectos relevantes.	**Nível de Confiança de 80%.** Os controles são capazes de mitigar 80% dos eventos. Risco de controle = 1,00 - 0,80.	0,20

* Não há controle perfeito. Todos têm limitações que impedem que NC seja igual a 1 (um). Por isto, não há RC < 0,20. Limitações do controle: relação custo-benefício; burla pela administração; conluio; erros de julgamento; falha humana (causada por fadiga, doença...); eventos externos.

O risco residual, então, é calculado como sendo o produto do risco inerente pelo risco de controle.

Risco Residual (RR) = Risco Inerente (RI) x Risco de Controle (RC)

Um bom exemplo é o risco de pagamento por serviço não executado ou executado parcialmente.

Devido à possibilidade de divergência entre o serviço contratado e o serviço efetivamente prestado, poderá ocorrer pagamento por serviço não executado ou executado parcialmente, gerando prejuízo financeiro e risco de responsabilização.

Considerando que a administração, na ausência de controles, poderia realizar o pagamento diretamente pela nota fiscal, esse risco pode ser entendido como um risco com alta probabilidade de ocorrência (8) e médio impacto (5), chegando a um risco inerente alto (8 x 8 = 40).

No entanto, esse risco pode ser fortemente reduzido se forem adotados controles, por exemplo:

- fiscal do contrato formalmente designado;
- ateste da execução antes do pagamento;
- checklist de conferência;

Esses controles podem ser entendidos como fortes (nível de confiança 80%). Assim, o risco residual será reduzido a níveis mais aceitáveis:

RR = 0,20.40 = 8

5.5. MONITORAMENTO

O monitoramento é contínuo e transversal, garantindo que os controles permaneçam eficazes. A estrutura de governança do TCE-PE responsável por este ciclo é,:

- **Estratégico:** Conselho de Governança Institucional (**CGI**).
- **Tático:** Comitê de Gestão de Riscos (**CGR**) – Coordenação pela DGG.
- **Operacional:** Subcomissão Temática de Gestão de Riscos (**STGR**) e Proprietários de Riscos (1ª Linha).
- **Apoio Metodológico (2ª Linha):** Gerência de Auditoria Interna (GAIN);
- **Avaliação Independente (3ª Linha):** Gerência de Auditoria Interna (GAIN).

O monitoramento não é apenas verificar se o risco aconteceu, mas acompanhar a eficácia da gestão. Deve ser realizado em três dimensões:

1. **Monitoramento do Sistema:** Verificar se a metodologia e o SGR (Sistema de Gestão de Riscos) estão funcionando adequadamente no setor.
2. **Monitoramento do Tratamento:** Verificar se as ações de resposta implementadas foram efetivas e reduziram o risco conforme esperado (risco residual).
3. **Monitoramento da Evolução:** Acompanhar a evolução dos níveis de riscos que *não* foram tratados (aceitos), para garantir que não saiam da faixa de tolerância ao longo do tempo.

5.6. COMUNICAÇÃO

A comunicação deve garantir que as informações fluam para subsidiar a tomada de decisão.

a. **Vertical:** é o fluxo de comunicação da operação para a gestão (CGI/CGR), e vice-versa. A informação deve subir da operação para a gestão, e, quando necessário, para as instâncias superiores quando envolver:
   - riscos acima da tolerância;
   - riscos críticos transversais, isto é, que afetam várias unidades e processos;
   - mudanças relevantes no risco (aumento de nível, novo risco relevante, falha de controle, incidentes significativos);
   - planos de tratamento em atraso ou com impedimentos;
   - decisões necessárias, como aceitação formal, priorização de recursos, mudança de processos, contratação de soluções etc.

b. **Horizontal:** é o fluxo de comunicação entre unidades no mesmo nível. É essencial em **Processos Transversais**, para tratar riscos que surgem em interfaces, dependências e cadeias de processos. Deve ser realizada a comunicação horizontal quando:
   - o tratamento de um risco depende de outra unidade (ex.: o tratamento de um risco na área de licitações depende de auxílio da TI);
   - o risco é transversal, isto é, impacta várias diretorias simultaneamente;
   - uma mudança de controle numa área aumenta o risco em outra.

6. REFERÊNCIAS BIBLIOGRÁFICAS

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise Risk Management** — Integrated Framework. [S. l.]: COSO, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: Gestão de riscos — Diretrizes. Rio de Janeiro: ABNT, 2018.

PERNAMBUCO. Tribunal de Contas do Estado (TCE-PE). **Portaria Normativa nº 285, de 20 de agosto de 2025**. Dispõe sobre a Política de Gestão de Riscos do Tribunal de Contas do Estado de Pernambuco (TCE-PE). Recife, PE, 2025. Disponível em: https://atosoficiais.com.br/tcepe/portaria-normativa-n-285-2025-dispoe-sobre-a-politica-de-gestao-de-riscos-do-tribunal-de-contas-do-estado-de-pernambuco-tce-pe?origin=instituicao. Acesso em: 22 de abr. 2026.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de Gestão de Riscos 2.0**. Brasília, DF: CGU, 2021. Disponível em: https://basedeconhecimento.cgu.gov.br/server/api/core/bitstreams/a1ecd91c-7df3-48db-8dfa-911b7e7c268b/content. Acesso em: 30 de mar. 2026.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos**. Brasília, DF: TCU, 2016. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/manual-de-gestao-de-riscos-do-tcu. Acesso em: 19 de abr. 2026.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos**: avaliação da maturidade. Brasília, DF: TCU, 2018. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/gestao-de-riscos-avaliacao-da-maturidade. Acesso em: 7 de ago. 2025.

GOIÁS. Tribunal de Justiça do Estado de Goiás (TJ-GO). **Manual de Gestão de Riscos**. Goiânia: TJ-GO, 2025. Disponível em: https://docs.tjgo.jus.br/institucional/gestaoestrategica/manual_gest%C3%A3o_riscos_2025_final.pdf. Acesso em: 23 de abr. 2026.

CEARÁ. Tribunal de Contas do Estado (TCE-CE). **Manual de Gestão de Riscos**. Fortaleza: TCE-CE, 2022. Disponível em: https://www.tce.ce.gov.br/downloads/manual_gestao_riscos_2022.pdf. Acesso em: 29 de abr. 2026.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). **Declaração de Posicionamento do IIA**: as três linhas de defesa no gerenciamento eficaz de riscos e controles. [S. l.]: IIA, 2013. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/as-trs-linhas-d-ippf-00000010-28082019095801.pdf. Acesso em: 06 de abr. 2026.

UNITED KINGDOM. National Audit Office (NAO). **Managing Risks in Government**. London: NAO, 2011. Disponível em:

https://www.nao.org.uk/wp-content/uploads/2011/06/managing_risks_in_government.pdf. Acesso em: 14 de ago. 2025.