Auditoria-Geral
do Município

Prefeitura de
SOROCABA

GUIA DE ELABORAÇÃO

PLANO DE GERENCIAMENTO DE RISCOS

Vol. 01 · 2ª edição · 2026

Guia de Elaboração – Plano de Gerenciamento de Riscos

Volume 01 · 2ª edição, revista e ampliada · Outubro de 2026

Elaboração: Auditoria-Geral do Município de Sorocaba

Novidades desta edição: inclusão da Parte II (gerenciamento de riscos nas contratações públicas – Lei nº 14.133/2021); glossário e base normativa; modelo das três linhas (art. 169); definição do apetite a risco; redação inequívoca das faixas de nível de risco; mapa de calor revisado; exemplos de cálculo; matriz de alocação de riscos; integração com o Assistente de matriz de riscos; abordagem didática, com caso prático, passo a passo, perguntas orientadoras, erros comuns e checklists em cada etapa; perguntas frequentes; referências bibliográficas.

Permitida a reprodução total ou parcial, desde que citada a fonte.

Como citar: SOROCABA. Auditoria-Geral do Município. Guia de elaboração: plano de gerenciamento de riscos. 2. ed. Sorocaba: Auditoria-Geral do Município, 2026. v. 1.

Sumário

Apresentação....4

PARTE I – Metodologia de gerenciamento de riscos 6

1. Conceitos fundamentais....7
2. Fundamentos normativos e responsabilidades....9
3. Visão geral do processo....11
4. Escolha dos objetos prioritários....13
5. Identificação de riscos....14
6. Análise e avaliação de riscos....19
7. Controle de riscos e risco residual....23
8. Tratamento dos riscos....26
9. Elaboração do plano de tratamento....29
10. Informação, comunicação e monitoramento....31

PARTE II – Gerenciamento de riscos nas contratações públicas 33

11. A gestão de riscos na Lei nº 14.133/2021....34
12. Riscos típicos por fase da contratação....37
13. Mapa de riscos e matriz de alocação de riscos....39
14. Ferramenta de apoio: Assistente de matriz de riscos....43
15. Perguntas frequentes....44

Conclusão....45
Referências....46
Anexo I – Estrutura do documento “Gestão de Riscos” (AG-9503)....47
Anexo II – Quadro-resumo....48

Apresentação

A gestão eficiente dos riscos é essencial para o bom funcionamento das atividades municipais, pois proporciona segurança administrativa, eficiência operacional e sustentabilidade institucional. Este guia oferece diretrizes claras e estruturadas para identificar, analisar, avaliar, tratar e monitorar riscos, de modo a garantir uma atuação preventiva e sistemática das unidades da Prefeitura de Sorocaba.

Esta 2ª edição amplia o conteúdo original em duas frentes. A **Parte I** consolida a metodologia de gerenciamento de riscos aplicável a qualquer processo, projeto ou objeto prioritário do Município. A **Parte II** aplica essa metodologia às contratações públicas, em atenção à Lei nº 14.133/2021, que tornou obrigatória a análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual (art. 18, X) e determinou que as contratações se submetam a práticas contínuas e permanentes de gestão de riscos e de controle preventivo (art. 169).

A edição também corrige e explicita pontos da versão anterior: as faixas de classificação do nível de risco passam a ter redação inequívoca, inclusive para valores decimais; o mapa de calor foi revisado; a referência normativa sobre apetite a risco foi atualizada; e foi definido o apetite a risco a ser observado pelas unidades.

> **Ferramenta de apoio**
>
> As etapas deste guia podem ser executadas no **Assistente de matriz de riscos**, ferramenta gratuita disponível em **auditoriageral.com.br**, que aplica automaticamente as escalas, fórmulas e regras aqui descritas e emite o documento padronizado “Gestão de Riscos” (AG-9503) para juntada ao processo no SEI (ver Capítulo 14).

Como usar este guia

Se você precisa…	Consulte
Entender os conceitos e a base normativa	Capítulos 1 e 2
Elaborar o Plano de Gerenciamento de Riscos de um processo ou projeto	Capítulos 3 a 10
Elaborar a análise de riscos de uma contratação (fase preparatória)	Capítulos 11 e 12, com a metodologia dos Capítulos 5 a 10
Elaborar a matriz de alocação de riscos de um contrato	Capítulo 13
Usar a ferramenta eletrônica	Capítulo 14
Ver um exemplo completo, do início ao fim	Quadros verdes “Caso prático”, nos Capítulos 3 a 13
Tirar dúvidas rápidas	Capítulo 15 – Perguntas frequentes
Consultar escalas e fórmulas rapidamente	Anexo II – Quadro-resumo

Como cada capítulo está organizado

Para facilitar o aprendizado de quem tem pouca familiaridade com o tema, os capítulos das etapas seguem a mesma estrutura:

Elemento	Para que serve
Em resumo	O que é a etapa, quem participa e qual o resultado esperado.
Conceitos e quadros	As regras e escalas da metodologia.
Passo a passo	A sequência prática de tarefas.
Caso prático	A aplicação da etapa em um caso fictício que acompanha todo o guia.
Erros comuns	Falhas frequentes e como evitá-las.
Antes de avançar, confirme	Lista de verificação para concluir a etapa com segurança.

PARTE I

Metodologia de gerenciamento de riscos

A Parte I descreve o processo de gerenciamento de riscos adotado pela Prefeitura de Sorocaba. A metodologia é aderente à ABNT NBR ISO 31000:2018 e às orientações do Tribunal de Contas da União (TCU), da Controladoria-Geral da União (CGU) e do Ministério do Planejamento e Orçamento (MPO), referências amplamente adotadas pela Administração Pública brasileira.

1. Conceitos fundamentais

Para que todas as unidades utilizem a mesma linguagem, adotam-se as definições a seguir.

Quadro 1 – Glossário

Termo	Definição	Fonte
Risco	Efeito da incerteza nos objetivos. No setor público, corresponde à possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.	ABNT NBR ISO 31000:2018; IN Conjunta MP/CGU nº 1/2016
Gestão de riscos	Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.	ABNT NBR ISO 31000:2018
Evento de risco	Incidente ou ocorrência, de fonte interna ou externa, que pode afetar negativamente os objetivos.	CGU (2018)
Causa	Condição que dá origem à possibilidade de ocorrência do evento. Resulta da combinação entre uma fonte de risco e uma vulnerabilidade.	CGU (2017)
Consequência	Resultado da ocorrência do evento que afeta os objetivos.	ABNT NBR ISO 31000:2018
Probabilidade	Chance de o evento acontecer, avaliada pela escala do Capítulo 6.	TCU (2017)
Impacto	Efeito resultante da ocorrência do evento sobre os objetivos, avaliado pela escala do Capítulo 6.	TCU (2017)
Risco inerente (RI)	Risco a que a organização está exposta sem considerar as ações gerenciais que possam reduzir sua probabilidade ou impacto.	TCU (2018)
Controle interno	Conjunto de regras, procedimentos, rotinas, sistemas e ações destinados a enfrentar os riscos e a dar razoável segurança ao alcance dos objetivos.	IN Conjunta MP/CGU nº 1/2016
Risco de controle (RC)	Parcela do risco que os controles existentes não conseguem mitigar; corresponde a 1 menos o nível de confiança nos controles.	MPO (2024)
Risco residual (RR)	Risco que permanece após considerados os controles existentes e que ainda requer tratamento específico.	TCU (2018); MPO (2024)
Apetite a risco	Quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir.	ABNT ISO Guia 73:2009; ISO 31073:2022
Plano de tratamento	Instrumento que detalha as ações para gerenciar os riscos, com responsáveis, prazos e recursos.	Este guia (Cap. 9)
Objeto Prioritário (OP)	Projeto ou processo selecionado para gestão de riscos segundo os critérios do Capítulo 4.	Este guia (Cap. 4)

Termo	Definição	Fonte
Mapa de riscos	Documento que registra a identificação, a análise e o tratamento dos riscos de uma contratação ao longo de suas fases.	TCU (2024)
Matriz de riscos	Cláusula contratual definidora de riscos e de responsabilidades entre as partes e caracterizadora do equilíbrio econômico-financeiro inicial do contrato.	Lei nº 14.133/2021, art. 6º, XXVII

2. Fundamentos normativos e responsabilidades

A gestão de riscos no setor público está ancorada em normas legais, regulamentos e padrões técnicos. O Quadro 2 reúne as principais referências utilizadas neste guia.

Quadro 2 – Principais referências normativas e técnicas

Norma ou referência	Conteúdo relevante
Lei nº 14.133/2021, art. 11, parágrafo único	A alta administração é responsável pela governança das contratações e deve implementar processos e estruturas, inclusive de gestão de riscos e controles internos.
Lei nº 14.133/2021, art. 18, X	A fase preparatória deve abordar a análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual.
Lei nº 14.133/2021, arts. 6º, XXVII, 22 e 103	Definem a matriz de riscos, sua obrigatoriedade e os critérios de alocação dos riscos entre contratante e contratado.
Lei nº 14.133/2021, art. 72, I	Nas contratações diretas, o processo é instruído, se for o caso, com análise de riscos.
Lei nº 14.133/2021, art. 169	As contratações submetem-se a práticas contínuas e permanentes de gestão de riscos e controle preventivo e às três linhas de defesa.
IN Conjunta MP/CGU nº 1/2016	Dispõe sobre controles internos, gestão de riscos e governança no Poder Executivo federal (referência técnica).
Decreto federal nº 9.203/2017	Política de governança da administração federal; trata a gestão de riscos como diretriz de governança (referência técnica).
ABNT NBR ISO 31000:2018	Princípios, estrutura e processo de gestão de riscos.
TCU – Referencial básico de gestão de riscos (2018) e Roteiro de auditoria de gestão de riscos (2017)	Conceitos, modelo de avaliação e escalas de probabilidade e impacto.
CGU – Metodologia de gestão de riscos (2018) e Manual de auditoria interna governamental (2017)	Processo de gestão de riscos e tabela de fontes de risco e vulnerabilidades.
MPO – Guia metodológico para gestão de riscos (2024)	Matriz de nível de risco e escala de avaliação preliminar dos controles.

2.1 Modelo das três linhas

O art. 169 da Lei nº 14.133/2021 organiza a gestão de riscos e o controle preventivo das contratações em três linhas de defesa, inspiradas no modelo do Instituto dos Auditores Internos (IIA, 2020). Cada linha tem um papel distinto e complementar:

Quadro 3 – Linhas de defesa nas contratações (art. 169)

Linha	Integrantes (art. 169)	Papel na gestão de riscos
1ª linha	Servidores e empregados públicos, agentes de licitação e autoridades que atuam na estrutura de governança do órgão.	Identificam, avaliam e tratam os riscos no dia a dia: elaboram o ETP, o termo de referência e o plano de gerenciamento de riscos, e executam e fiscalizam o contrato.
2ª linha	Unidades de assessoramento jurídico e de controle interno do próprio órgão.	Apoiam e supervisionam a 1ª linha: orientam, revisam a análise de riscos e verificam a adequação dos controles.
3ª linha	Órgão central de controle interno da Administração e tribunal de contas.	Avaliam de forma independente a eficácia da gestão de riscos e dos controles. No Município, essa avaliação cabe à Auditoria-Geral do Município, como órgão central de controle interno, e ao Tribunal de Contas do Estado de São Paulo.

Responsabilidade da alta administração

A implementação das práticas de gestão de riscos é responsabilidade da alta administração, que deve considerar os custos e os benefícios dessas práticas e optar pelas medidas que promovam relações íntegras e confiáveis, com segurança jurídica e o resultado mais vantajoso para a Administração (art. 169, §1º).

3. Visão geral do processo

Em resumo

O que é: o roteiro completo, em sete etapas, para elaborar e manter um Plano de Gerenciamento de Riscos.

Quem participa: a unidade responsável pelo processo ou pela contratação, com apoio da 2ª linha quando necessário.

Resultado esperado: uma visão clara do caminho a percorrer antes de começar o trabalho.

O gerenciamento de riscos é um processo contínuo, desenvolvido em sete etapas. As etapas 2 a 6 compõem o núcleo técnico do Plano de Gerenciamento de Riscos; a etapa 7 permeia todo o processo.

Quadro 4 – Etapas do gerenciamento de riscos

Etapa	O que fazer	Produto	Cap.
1. Escolha dos objetos prioritários	Selecionar os projetos ou processos sujeitos à gestão de riscos.	Lista de OPs justificada	4
2. Identificação	Levantar eventos de risco, causas e consequências.	Tabela de identificação	5
3. Análise e avaliação	Atribuir probabilidade e impacto e calcular o risco inerente.	Risco inerente e mapa de calor	6
4. Controle	Avaliar os controles existentes e calcular o risco residual.	Risco residual	7
5. Tratamento	Escolher a resposta a cada risco conforme o apetite a risco.	Resposta definida	8
6. Plano de tratamento	Detalhar ações, responsáveis, prazos e recursos.	Plano de tratamento aprovado	9
7. Informação, comunicação e monitoramento	Comunicar, registrar no SEI e acompanhar periodicamente.	Registros de monitoramento	10

3.1 Como organizar o trabalho

Antes de preencher qualquer tabela, vale organizar o trabalho. Uma análise de riscos feita por uma única pessoa, às pressas, tende a listar riscos genéricos e a atribuir notas sem fundamento. Recomenda-se:

1. **Forme a equipe.** Reúna de três a seis pessoas que conheçam o processo de ângulos diferentes – por exemplo, quem demanda, quem especifica, quem compra e quem fiscaliza.
2. **Reúna os insumos.** Separe o processo anterior do mesmo objeto (se houver), relatórios de fiscalização, notificações e sanções aplicadas, apontamentos de auditoria e do TCE-SP, reclamações de usuários e a minuta do ETP ou do termo de referência.
3. **Marque uma oficina.** Uma reunião de 90 a 120 minutos costuma bastar para identificar os riscos e discutir as notas. Use a tabela de identificação (Quadro 8) ou a ferramenta eletrônica projetada na tela.

4. **Conclua e valide.** Após a oficina, um responsável consolida o documento, completa o plano de tratamento e o submete à validação do gestor máximo da unidade.
5. **Registre e acompanhe.** Junte o documento ao processo no SEI e agende o primeiro monitoramento.

3.2 O caso prático deste guia

Para mostrar como cada etapa funciona na prática, este guia acompanha, do Capítulo 4 ao 13, um **caso fictício**, apresentado em quadros verdes como o abaixo. Os números e situações são ilustrativos.

> **Caso prático – apresentação**
>
> A **Secretaria da Saúde** precisa contratar **serviços contínuos de limpeza, conservação e higienização, com dedicação exclusiva de mão de obra**, para 30 unidades básicas de saúde. O valor estimado é de **R$ 4,8 milhões por ano**; a contratação será feita por **pregão eletrônico**, em regime de **empreitada por preço global**, com vigência de 12 meses, prorrogável.
>
> No contrato anterior, os relatórios de fiscalização registraram faltas frequentes de empregados sem reposição, e houve reclamações trabalhistas de ex-empregados da empresa contratada.

4. Escolha dos objetos prioritários

Em resumo

O que é: a decisão sobre quais processos, projetos ou contratações terão seus riscos gerenciados formalmente.

Quem participa: dirigentes da unidade e equipe técnica.

Resultado esperado: uma lista de objetos prioritários com a justificativa de cada escolha.

Preliminarmente, devem ser identificados os projetos ou processos prioritários (Objetos Prioritários – OPs) sujeitos à gestão de riscos, observados os critérios abaixo. Basta que o objeto atenda a um dos critérios, devendo a escolha ser justificada.

Quadro 5 – Critérios de seleção dos objetos prioritários

Critério	Descrição
Materialidade	Projetos cuja execução envolva montantes financeiros significativos, afetando substancialmente o orçamento e as contas públicas municipais.
Criticidade	Projetos com histórico frequente de irregularidades detectadas por órgãos internos e externos de controle ou por auditorias internas.
Relevância	Projetos diretamente alinhados aos objetivos estratégicos definidos pelo Plano Estratégico Institucional vigente.
Inovação	Projetos com potencial transformador, que exijam elevado grau de inovação tecnológica, metodológica ou administrativa.

Contratações

Nas contratações públicas, a análise de riscos é obrigatória independentemente desses critérios (art. 18, X, da Lei nº 14.133/2021). Os critérios de priorização servem, nesse caso, para dimensionar a profundidade da análise e para registrar, no documento, as características que tornam a contratação sensível.

Caso prático – escolha do objeto

A contratação de limpeza atende a três critérios:

Materialidade: R$ 4,8 milhões por ano, um dos maiores contratos de serviços da Secretaria.

Criticidade: histórico de faltas sem reposição e de reclamações trabalhistas no contrato anterior.

Relevância: a higienização das unidades de saúde é essencial à segurança sanitária dos pacientes.

Justificativa registrada: “Contratação de alta materialidade, com histórico de falhas de execução e impacto direto na segurança sanitária das unidades de saúde.”

Erros comuns – evite

- ✕ Marcar todos os critérios sem justificar nenhum.
- ✕ Deixar de fazer a análise de riscos de uma contratação porque ela “não é prioritária” – nas contratações, a análise é obrigatória (art. 18, X); os critérios apenas indicam a profundidade necessária.

5. Identificação de riscos

Em resumo

O que é: o levantamento dos eventos que podem atrapalhar o alcance dos objetivos, com suas causas e consequências.

Quem participa: todos os que conhecem o processo: quem planeja, quem executa, quem fiscaliza e, se possível, quem já viveu problemas em situações semelhantes.

Resultado esperado: a tabela de identificação de riscos (Quadro 8) preenchida.

A identificação dos riscos deve envolver todos os agentes relacionados ao processo, desde o planejamento até a supervisão, garantindo abrangência no levantamento dos riscos relevantes. Podem ser utilizadas técnicas como reuniões de brainstorming, entrevistas com os executores, listas de verificação, análise de processos semelhantes e consulta a achados de auditoria e a apontamentos do Tribunal de Contas do Estado de São Paulo (TCE-SP).

5.1 Classificação dos riscos

Quadro 6 – Categorias de risco

Categoria	Definição
Estratégicos	Decorrentes de decisões gerenciais que influenciam diretamente os objetivos estratégicos.
Operacionais	Resultantes de falhas ou deficiências em processos internos, recursos humanos, infraestrutura física e tecnológica ou sistemas utilizados pelo Município.
Conformidade	Associados ao descumprimento ou a mudanças legislativas ou normativas que possam comprometer as atividades municipais.
Integridade	Relacionados a fraudes, corrupção ou desvios éticos e de conduta que prejudiquem os valores institucionais e a consecução dos objetivos estratégicos e operacionais.

5.2 Causas: fontes e vulnerabilidades

A causa de um risco resulta da combinação de uma **fonte de risco** com uma **vulnerabilidade**: **Causa = Fonte + Vulnerabilidade**. O Quadro 7 orienta a busca das causas.

Quadro 7 – Fontes de risco e vulnerabilidades

Fonte de risco	Vulnerabilidades
Pessoas	Em número insuficiente; sem capacitação; perfil inadequado; desmotivadas; alta rotatividade; propensas a desvios éticos e/ou fraudes.
Processos	Mal concebidos (exemplo: fluxo, desenho); sem manuais ou instruções formalizadas (procedimentos, documentos padronizados); sem segregação de funções; sem transparência.
Sistemas	Obsoletos; sem manuais de operação; sem integração com outros sistemas; inexistência de controles de acesso lógico e de backups; baixo grau de automação. Infraestrutura física e localização inadequadas; instalações ou leiaute inadequados; inexistência de controles de acesso físico.
Tecnologia	Técnica ultrapassada ou produto obsoleto; falta de investimento em TI; tecnologia sem proteção de patentes; processo produtivo sem proteção contra espionagem; controles insuficientes sobre a transferência de dados.
Eventos externos	**Ambientais:** mudança climática brusca, incêndio, inundação, epidemia. **Econômicos:** oscilações de juros, de câmbio e de preços; contingenciamento; queda de arrecadação; crise de credibilidade; elevação ou redução da carga tributária. **Políticos:** novas leis e regulamentos; restrição de acesso a mercados estrangeiros; ações de responsabilidade de outros gestores; “guerra fiscal” entre estados; conflitos; divergências diplomáticas. **Sociais:** alterações nas condições sociais e demográficas ou nos costumes; alterações nas demandas sociais; paralisações; aumento do desemprego. **Tecnológicos:** novas formas de comércio eletrônico; alterações na disponibilização de dados; variação do custo de infraestrutura; aumento da demanda por serviços baseados em tecnologia; ataques cibernéticos. **Infraestrutura:** conservação das vias de acesso; distância de portos e aeroportos; interrupções e aumentos de tarifa de água, energia elétrica e telefonia. **Legais/jurídicos:** novas leis e normas reguladoras; novos regulamentos; alterações na jurisprudência dos tribunais; ações judiciais.
Governança	Competências e responsabilidades não identificadas ou desrespeitadas; centralização ou descentralização excessiva; delegações exorbitantes; falta de estratégia de controle; deficiência nos fluxos de informação e comunicação; informações para a tomada de decisão incompletas, imprecisas ou obscuras; pressão competitiva; falta de rodízio de pessoal; falta de formalização de instruções.
Planejamento	Ausência de planejamento; planejamento elaborado sem embasamento técnico ou em desacordo com as normas vigentes; objetivos e estratégias inadequados ou em desacordo com a realidade.

Fonte: CGU, Manual de orientações técnicas da atividade de auditoria interna governamental do Poder Executivo Federal, 2017 (adaptado).

5.3 Como descrever o risco

Recomenda-se descrever cada risco em uma frase que encadeie causa, evento e consequência, o que facilita a análise e a escolha das medidas de tratamento:

> "**Devido a** [causa], **poderá ocorrer** [evento], **o que levaria a** [consequência]."
>
> *Exemplo:* Devido à ausência de série histórica de consumo (causa), poderá ocorrer estimativa de quantidades superdimensionada (evento), o que levaria a desperdício de recursos e a aditivos desnecessários (consequência).

Os riscos identificados devem ser registrados conforme o modelo do Quadro 8. Caso dois eventos ou consequências tenham a mesma causa, devem ser agrupados como um mesmo risco.

Quadro 8 – Modelo de tabela de identificação de riscos

Nº	Evento de risco	Categoria	Possíveis causas	Possíveis consequências
R1	Descrever o incidente ou ocorrência que pode afetar negativamente os objetivos.	Estratégico, Operacional, Conformidade ou Integridade	Fonte + vulnerabilidade que, individualmente ou combinadas, podem dar origem ao risco.	Resultados da ocorrência do risco que impactam o objetivo.
R2				

Fonte: adaptado de MPO (2024).

5.4 Passo a passo da identificação

1. **Defina o objetivo.** Escreva em uma frase o que o processo ou a contratação precisa alcançar. Risco é tudo aquilo que pode impedir esse objetivo. *Exemplo:* "Manter as 30 unidades de saúde limpas e higienizadas, todos os dias, ao menor custo e sem passivos para a Prefeitura."
2. **Percorra as fases.** Pense no que pode dar errado em cada momento – planejamento, execução, encerramento – usando as perguntas do quadro a seguir.
3. **Busque as causas.** Para cada evento levantado, pergunte "por que isso aconteceria?" e use o Quadro 7 (fontes e vulnerabilidades) para não esquecer nenhuma origem.
4. **Descreva as consequências.** Pergunte "se acontecer, o que isso provoca?" – atraso, custo maior, serviço ruim, dano à imagem, responsabilização.
5. **Escreva a frase do risco** na estrutura "Devido a…, poderá ocorrer…, o que levaria a…".
6. **Classifique** cada risco em uma das quatro categorias (Quadro 6).
7. **Agrupe e revise.** Junte riscos com a mesma causa, elimine repetições e descarte o que não é risco (ver dica abaixo).

Perguntas orientadoras para a identificação

Fase	Perguntas
Planejamento	A necessidade está bem definida e documentada? As quantidades têm memória de cálculo baseada em dados? O preço estimado tem fontes suficientes e confiáveis? Há dotação orçamentária e previsão no plano de contratações anual? O prazo até a contratação é suficiente?
Seleção do fornecedor	As exigências do edital restringem a competição sem necessidade? Há poucos fornecedores capazes de atender? Há sinais de combinação entre licitantes? Como saber se uma proposta muito baixa é exequível?
Execução e encerramento	Há gestor e fiscais designados e capacitados? Como a execução será medida e comprovada? O que acontece se a contratada atrasar ou falhar? Há obrigações trabalhistas ou previdenciárias envolvidas? Os preços podem variar durante o contrato? O que pode dar errado no encerramento (verbas rescisórias, transição para novo contrato)?

Dica

Risco não é problema. Risco é um evento **futuro e incerto**; problema é algo que **já está acontecendo**. Se as faltas de empregados já ocorrem hoje, o problema atual deve ser resolvido pela gestão do contrato vigente, e o risco a registrar é que elas **voltem a ocorrer** no novo contrato. Também não é risco a simples ausência de uma medida (“falta de fiscalização”): a ausência é a **causa**; o risco é o evento que ela provoca (pagamento sem comprovação da execução).

Caso prático – riscos identificados

Na oficina com a área demandante, o fiscal do contrato anterior e a área de compras, a equipe identificou, entre outros, os quatro riscos abaixo:

Nº	Frase do risco	Categoria
R1	Devido à ausência de conferência sistemática da folha, do FGTS e do INSS, poderá ocorrer inadimplemento trabalhista e previdenciário da contratada, o que levaria à responsabilização da Prefeitura (art. 121, §2º) e a passivo trabalhista.	Conformidade
R2	Devido ao uso de convenção coletiva desatualizada e a encargos calculados sem revisão, poderá ocorrer erro na planilha de custos, o que levaria a preço estimado inexequível ou com sobrepreço.	Operacional
R3	Devido à falta de reserva técnica da contratada e ao controle de frequência em papel, poderão ocorrer postos de trabalho descobertos, o que levaria a unidades sem higienização adequada e a pagamento por posto não ocupado.	Operacional

Nº	Frase do risco	Categoria
R4	Devido à designação informal de fiscais com acúmulo de contratos, poderá ocorrer fiscalização deficiente, o que levaria a pagamentos sem comprovação da execução.	Operacional

Erros comuns – evite

- ✕ Listar riscos genéricos que servem para qualquer contratação (“risco de corrupção”, “risco de atraso”) sem dizer por que poderiam ocorrer neste caso.
- ✕ Confundir causa, evento e consequência na mesma frase ou registrar apenas o evento.
- ✕ Identificar dezenas de riscos irrelevantes e deixar de lado os poucos que realmente importam.
- ✕ Fazer a identificação sozinho, sem ouvir quem executa ou fiscaliza.

Antes de avançar, confirme

- ✓ Cada risco tem evento, causa (fonte + vulnerabilidade) e consequência.
- ✓ Os riscos são específicos do objeto analisado.
- ✓ Riscos com a mesma causa foram agrupados.
- ✓ Todas as fases foram consideradas.
- ✓ Cada risco tem uma categoria.

6. Análise e avaliação de riscos

Em resumo

O que é: a medição de cada risco, atribuindo uma nota de probabilidade e uma de impacto e multiplicando-as.

Quem participa: a mesma equipe da identificação, preferencialmente reunida, para que as notas sejam discutidas e não atribuídas por uma única pessoa.

Resultado esperado: o risco inerente de cada risco, sua classificação (baixo, médio, alto ou extremo) e o mapa de calor.

Após a identificação, cada risco deve ser analisado pela combinação de sua probabilidade de ocorrência com o impacto potencial sobre os objetivos. O produto das duas notas é o **risco inerente**:

Risco Inerente (RI) = Probabilidade × Impacto

Quadro 9 – Escala de probabilidade

Magnitude	Descrição	Nota
Muito baixa	**Evento improvável de ocorrer.** Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade.	**1**
Baixa	**Evento raro de ocorrer.** O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	**2**
Média	**Evento possível de ocorrer.** Há elementos e/ou informações que indicam moderadamente essa possibilidade.	**5**
Alta	**Evento provável de ocorrer.** É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	**8**
Muito alta	**Evento praticamente certo de ocorrer.** Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	**10**

Fonte: TCU, Roteiro de Auditoria de Gestão de Riscos, 2017 (adaptado).

Quadro 10 – Escala de impacto

Magnitude	Descrição	Nota
Muito baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causando **impactos mínimos nos objetivos** de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos e serviços às partes interessadas.	**1**
Baixo	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos pequenos nos objetivos**.	**2**
Médio	Interrupção de operações ou atividades de processos, projetos ou programas, causando **impactos significativos nos objetivos, porém recuperáveis**.	**5**
Alto	Interrupção de operações ou atividades de processos, projetos ou programas da organização, causando **impactos de reversão muito difícil nos objetivos**.	**8**
Muito alto	Paralisação de operações ou atividades de processos, projetos ou programas da organização, causando **impactos irreversíveis ou catastróficos nos objetivos**.	**10**

Fonte: TCU, Roteiro de Auditoria de Gestão de Riscos, 2017 (adaptado).

6.1 Classificação do nível de risco

O resultado do produto é classificado em quatro níveis. A mesma classificação vale para o risco inerente e para o risco residual (Capítulo 7).

Quadro 11 – Níveis de risco

Nível de risco	Resultado do produto
Baixo	Até 9
Médio	Acima de 9 até 39
Alto	Acima de 39 até 79
Extremo	A partir de 80

Fonte: adaptado de MPO (2024).

Valores decimais, que podem surgir no cálculo do risco residual, seguem a mesma regra: um resultado de 9,6, por exemplo, está **acima de 9** e é classificado como **Médio**.

Quadro 12 – Mapa de calor (Probabilidade × Impacto)

10 – Muito alto	**10**	**20**	**50**	**80**	**100**
8 – Alto	**8**	**16**	**40**	**64**	**80**
5 – Médio	**5**	**10**	**25**	**40**	**50**
2 – Baixo	**2**	**4**	**10**	**16**	**20**
1 – Muito baixo	**1**	**2**	**5**	**8**	**10**
Impacto ↑ / Probabilidade →	**1 – Muito baixa**	**2 – Baixa**	**5 – Média**	**8 – Alta**	**10 – Muito alta**

Fonte: adaptado de MPO (2024). Cores conforme o Quadro 11.

6.2 Passo a passo da análise

1. **Avalie a probabilidade.** Pergunte: isso já aconteceu antes, aqui ou em situações parecidas? Com que frequência? Há sinais de que pode acontecer agora? Escolha a nota pela descrição do Quadro 9 que melhor corresponde às evidências.
2. **Avalie o impacto.** Pergunte: se acontecer, o que é afetado – prazo, custo, qualidade, atendimento à população, imagem, conformidade legal? O dano é reversível? Escolha a nota pela descrição do Quadro 10.
3. **Multiplique** as duas notas para obter o risco inerente e classifique-o pelo Quadro 11.
4. **Registre o porquê.** Anote em uma linha a razão de cada nota. Isso torna a análise verificável e facilita revisões futuras.
5. **Visualize no mapa de calor** (Quadro 12) e confira se a posição de cada risco faz sentido para a equipe.

Dica

Avalie o risco como se nada estivesse sendo feito. Nesta etapa, ignore os controles existentes – eles entram no Capítulo 7. Use somente as notas 1, 2, 5, 8 e 10; notas intermediárias (3, 4, 6…) não existem na escala. E desconfie quando todos os riscos receberem nota "Média": geralmente é sinal de que a discussão não aprofundou as evidências.

Caso prático – análise do risco inerente

Risco	Probabilidade (por quê)	Impacto (por quê)	RI
R1	**Média (5)** – houve reclamações trabalhistas no contrato anterior.	**Alto (8)** – responsabilização da Prefeitura, de reversão muito difícil.	**40 Alto**
R2	**Baixa (2)** – a equipe usa ferramenta de cálculo; erros são raros.	**Alto (8)** – preço errado compromete toda a licitação.	**16 Médio**
R3	**Alta (8)** – faltas sem reposição registradas com frequência no contrato atual.	**Médio (5)** – prejudica o serviço, mas é recuperável com reposição.	**40 Alto**
R4	**Média (5)** – fiscais acumulam contratos.	**Alto (8)** – pagamentos indevidos e dano ao erário.	**40 Alto**

Erros comuns – evite

- ✕ Considerar os controles existentes já nesta etapa, o que subestima o risco.
- ✕ Atribuir notas sem registrar a justificativa.
- ✕ Usar notas fora da escala (3, 4, 6, 7, 9).
- ✕ Confundir impacto alto com probabilidade alta: um evento grave pode ser raro, e vice-versa.

Antes de avançar, confirme

- ✔ Cada risco tem nota de probabilidade e de impacto, com a justificativa registrada.
- ✔ O risco inerente foi calculado e classificado.
- ✔ O mapa de calor foi conferido pela equipe.

7. Controle de riscos e risco residual

Em resumo

O que é: a verificação de quanto os controles que já funcionam hoje reduzem cada risco.

Quem participa: a equipe técnica e quem executa os controles na prática.

Resultado esperado: o risco residual de cada risco, que indica o que ainda precisa ser tratado.

Apurado o risco inerente, ele deve ser confrontado com as estruturas vigentes de controle interno, a fim de determinar o **risco residual** – aquele que ainda necessita de tratamento específico por parte da Administração. Avaliam-se apenas os controles **já implantados**; medidas novas são definidas no tratamento (Capítulos 8 e 9).

Risco Residual (RR) = Risco Inerente × Risco de Controle

Quadro 13 – Escala de avaliação preliminar dos controles

Avaliação do controle	Situação do controle existente	Nível de confiança (NC)	Risco de controle (RC = 1 − NC)
Inexistente	Controle não existe, não funciona ou não está implementado.	Nenhum	**1,00**
Fraco	Controle não institucionalizado; está na esfera de conhecimento pessoal dos operadores do processo; em geral realizado de maneira manual.	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.	40%	**0,60**
Satisfatório	Controle institucionalizado e, embora passível de aperfeiçoamento, sustentado por ferramentas adequadas; mitiga o risco razoavelmente.	60%	**0,40**
Forte	Controle institucionalizado e sustentado por ferramentas adequadas, podendo ser considerado “melhor prática”; mitiga o risco em todos os aspectos relevantes.	80%	**0,20**

Fonte: MPO (2024). Não há controle perfeito: todos têm limitações que impedem que o nível de confiança seja igual a 100%.

O risco residual é classificado pelos mesmos níveis do Quadro 11.

Quadro 14 – Exemplos de cálculo

Risco	P	I	RI	Controle (RC)	RR	Nível residual
Estimativa de quantidades sem memória de cálculo	5	8	40	Fraco (0,80)	32	Médio
Pagamento sem conferência da execução	8	10	80	Mediano (0,60)	48	Alto
Planilha de custos com erros	2	8	16	Mediano (0,60)	9,6	Médio (acima de 9)
Pessoalidade na gestão de terceirizados	2	2	4	Forte (0,20)	0,8	Baixo

7.1 Passo a passo da avaliação dos controles

1. **Liste os controles que existem hoje** para cada risco: normas, rotinas, checklists, sistemas, conferências, segregação de funções, cláusulas contratuais padronizadas.
2. **Verifique se funcionam na prática.** Um controle previsto em norma, mas que ninguém executa, é "Inexistente". Peça evidências: registros, relatórios, telas de sistema.
3. **Classifique cada controle** pela escala do Quadro 13, com apoio do roteiro abaixo.
4. **Calcule o risco residual** multiplicando o risco inerente pelo risco de controle e classifique-o pelo Quadro 11.

Roteiro de apoio para classificar o controle

Pergunta	Se a resposta for…	Classificação provável
O controle existe e é efetivamente executado?	Não	Inexistente (1,00)
Ele está escrito em norma, rotina ou checklist?	Não; depende da iniciativa de quem executa	Fraco (0,80)
Ele cobre todos os aspectos relevantes do risco?	Está formalizado, mas deixa lacunas ou às vezes falha	Mediano (0,60)
Há ferramenta adequada e evidência de execução regular?	Sim, embora possa ser aperfeiçoado	Satisfatório (0,40)
Ele é automatizado ou tem dupla verificação, cobre todos os aspectos e é referência de boa prática?	Sim	Forte (0,20)

Roteiro de apoio elaborado para este guia, com base nas descrições do Quadro 13.

Caso prático – avaliação dos controles e risco residual

Risco	Controle existente	Avaliação	RI	RR
R1	Exigência mensal de comprovantes, conferidos manualmente pelo fiscal, sem roteiro.	Fraco (0,80)	**40**	**32 Médio**

Risco	Controle existente	Avaliação	RI	RR
R2	Planilha revisada pelo chefe da divisão com checklist formal e ferramenta de cálculo.	Satisfatório (0,40)	**16**	**6,4 Baixo**
R3	Controle de frequência em papel, sem glosa prevista no contrato.	Fraco (0,80)	**40**	**32 Médio**
R4	Nenhum: os fiscais são indicados informalmente.	Inexistente (1,00)	**40**	**40 Alto**

Erros comuns – evite

- ✕ Considerar como existente um controle que ainda será implantado – ele pertence ao plano de tratamento.
- ✕ Classificar como “Forte” um controle sem evidência de que funciona.
- ✕ Esquecer que nenhum controle elimina o risco por completo (o melhor fator é 0,20).

Antes de avançar, confirme

- ✓ Cada risco tem seus controles existentes descritos, ou a indicação de que não há controle.
- ✓ A classificação do controle tem evidência que a sustente.
- ✓ O risco residual foi calculado e classificado.

8. Tratamento dos riscos

Em resumo

O que é: a escolha do que fazer com cada risco residual: aceitar, mitigar, transferir ou evitar.

Quem participa: a equipe técnica, que propõe, e o gestor máximo da unidade, que valida.

Resultado esperado: uma resposta definida e justificada para cada risco, respeitando o apetite a risco.

Os riscos devem ser tratados considerando sua natureza, o impacto potencial e a tolerância da Administração. As estratégias de tratamento são:

Quadro 15 – Estratégias de tratamento

Estratégia	Descrição
Aceitar	Não adotar medidas, dado que o risco residual é baixo ou o custo da mitigação é superior aos benefícios. As justificativas devem ser comunicadas claramente à alta administração.
Mitigar	Implementar medidas que reduzam a probabilidade e/ou o impacto.
Transferir ou compartilhar	Reduzir o risco transferindo-o parcialmente para terceiros, como seguradoras ou prestadores terceirizados.
Evitar	Cessar ou impedir as atividades geradoras do risco, eliminando sua possibilidade.

8.1 Seleção da alternativa de tratamento

Para selecionar a alternativa mais adequada, recomenda-se:

1. **Verificação do custo-benefício:** analisar a relação custo-benefício de cada alternativa, considerando seu efeito sobre a probabilidade e o impacto do risco, os casos em que o tratamento não seja economicamente justificável e os possíveis riscos secundários resultantes das medidas adotadas.
2. **Elaboração do plano de tratamento:** desenvolver um plano de ação detalhado e específico para cada risco, contemplando a opção selecionada (Capítulo 9).
3. **Validação dos controles:** submeter os planos de tratamento ao gestor máximo da unidade para análise e validação quanto à viabilidade econômica e operacional, priorizando-se os que serão efetivamente executados.
4. **Observância do apetite a risco:** respeitar o nível de risco aceitável definido na seção 8.2.

8.2 Apetite a risco

Apetite a risco é a “quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir” (ABNT ISO Guia 73:2009; ISO 31073:2022). Com base em um nível de exposição predefinido, a organização consegue antecipar-se e prever planos de mitigação e correção mais adequados. Fica estabelecido o seguinte apetite a risco:

Quadro 16 – Apetite a risco da Prefeitura de Sorocaba

Risco residual	Diretriz	Exigência
Baixo	Pode ser aceito.	Registrar a justificativa da aceitação.
Médio	Pode ser aceito mediante justificativa; recomenda-se mitigar.	Justificativa fundamentada e comunicada à alta administração.
Alto	Não pode ser aceito; tratamento obrigatório.	Plano de tratamento com ações, responsáveis e prazos.
Extremo	Não pode ser aceito; tratamento obrigatório e prioritário.	Plano de tratamento e comunicação imediata à alta administração.

8.3 Passo a passo do tratamento

1. **Ordene os riscos** do maior para o menor risco residual. Comece pelos extremos e altos.
2. **Aplique o apetite a risco** (Quadro 16): riscos altos e extremos não podem ser aceitos; riscos médios só podem ser aceitos com justificativa.
3. **Escolha a estratégia** mais adequada (Quadro 15), comparando custo e benefício. Pergunte: a medida reduz a probabilidade, o impacto ou ambos? Quanto custa? Cria novos riscos?
4. **Justifique** toda aceitação, em especial a de riscos médios.
5. **Submeta à validação** do gestor máximo da unidade.

Exemplos de medidas por estratégia, em contratações

Estratégia	Exemplos
Mitigar	Memória de cálculo das quantidades; cesta de preços ampliada; roteiro e capacitação da fiscalização; instrumento de medição de resultado; cláusula de glosa; conta-depósito vinculada.
Transferir ou compartilhar	Exigência de seguro (responsabilidade civil, riscos de engenharia); garantia contratual; alocação do risco à contratada na matriz de riscos.
Evitar	Mudar o desenho da contratação – por exemplo, dividir o objeto em lotes, alterar o regime de execução ou deixar de contratar uma parcela de alto risco.
Aceitar	Riscos baixos, ou médios cujo tratamento custe mais do que o benefício, com justificativa registrada.

Caso prático – respostas escolhidas

Risco	RR	Resposta	Justificativa
R1	**32 Médio**	Mitigar	Embora possa ser aceito, o impacto é grave e há medida eficaz e de baixo custo (conta-depósito vinculada).
R2	**6,4 Baixo**	Aceitar	Controles atuais satisfatórios; nova medida não traria benefício relevante.
R3	**32 Médio**	Mitigar	Histórico de ocorrência; cláusula de reposição e glosa tem custo baixo.

Risco	RR	Resposta	Justificativa
R4	**40 Alto**	Mitigar	Risco alto: tratamento obrigatório pelo apetite a risco.

Erros comuns – evite

- ✕ Aceitar riscos altos ou extremos.
- ✕ Aceitar riscos sem justificativa.
- ✕ Escolher medidas que não têm relação com a causa do risco.
- ✕ Propor medidas que a unidade não tem condições de executar.

9. Elaboração do plano de tratamento

Em resumo

O que é: o detalhamento, risco a risco, do que será feito, por quem, até quando e com quais recursos.

Quem participa: a equipe técnica e os responsáveis pelas ações.

Resultado esperado: o plano de tratamento aprovado e juntado ao processo no SEI.

O **Plano de Tratamento** é o instrumento estruturado que detalha, de forma clara e objetiva, as ações específicas necessárias para gerenciar adequadamente os riscos identificados, atribuindo expressamente sua implementação a um responsável ou equipe designada. Um plano eficaz permite abordagem preventiva, em oposição à reativa, e garante resposta célere e eficiente diante de eventual materialização do risco.

Sugere-se às unidades administrativas o seguinte roteiro:

1. **Definição das ações e controles:** indicar, de forma objetiva, as ações a serem adotadas – mitigação, salvaguardas ou preparação para cenários futuros –, especificando se envolvem projetos, melhorias de sistemas, criação ou revisão de normas, planos de contingência ou outras ações correlatas. **É imprescindível demonstrar a correlação lógica entre a ação proposta e seus efeitos sobre o risco identificado.**
2. **Atribuição de responsabilidades:** estabelecer quem será responsável pela implementação de cada ação, indicando a Secretaria, a unidade administrativa pertinente e o gestor ou a autoridade designada, e esclarecer se haverá envolvimento de outras áreas ou servidores e como ocorrerá essa participação.
3. **Estabelecimento de prazos e metas:** definir as tarefas necessárias, com prazos de início e conclusão, cronograma formalizado e metas claras e alcançáveis para cada etapa.
4. **Determinação dos recursos necessários:** identificar os recursos financeiros, humanos e materiais indispensáveis, verificando se já estão disponíveis ou se haverá necessidade de aporte adicional ou realocação, e esclarecer como serão providenciados.

Quadro 17 – Campos mínimos do plano de tratamento (por risco)

Campo	Conteúdo esperado
Risco e nível residual	Identificação do risco (R1, R2…) e classificação do risco residual.
Resposta	Aceitar, mitigar, transferir/compartilhar ou evitar; justificativa quando aceito.
Ações e controles propostos	O que será feito.
Correlação lógica	Como a ação reduz a probabilidade e/ou o impacto do risco.
Plano de contingência	O que fazer se o risco se materializar.
Responsáveis	Unidade responsável, gestor ou autoridade designada e áreas envolvidas.
Prazos e metas	Início, conclusão, tarefas e metas.
Recursos	Recursos necessários, disponibilidade e forma de obtenção.

Após a aprovação formal, o plano deve ser amplamente divulgado e comunicado a todas as partes interessadas, especialmente à alta administração.

Caso prático – plano de tratamento do risco R4

Campo	Conteúdo
Risco e nível residual	R4 – Fiscalização deficiente · Alto (40)
Resposta	Mitigar
Ações e controles propostos	1) Publicar portaria de designação do gestor e de dois fiscais (técnico e administrativo) antes da assinatura do contrato. 2) Capacitar os fiscais em fiscalização de serviços com mão de obra. 3) Adotar roteiro mensal de fiscalização, com relatório anexado a cada ateste.
Correlação lógica	A designação formal e a capacitação atacam a causa (fiscais informais e sem preparo); o roteiro com relatório obrigatório reduz a probabilidade de pagamento sem comprovação.
Plano de contingência	Se for constatado pagamento indevido: glosa na fatura seguinte, notificação da contratada e apuração de responsabilidade.
Responsáveis	Divisão de Contratos da Secretaria da Saúde; gestora designada: chefe da Divisão; apoio da área de capacitação.
Prazos e metas	Início: data da homologação. Conclusão: até a assinatura do contrato (portaria) e em 60 dias (capacitação). Meta: 100% dos atestes com relatório de fiscalização.
Recursos	Horas de trabalho da equipe; curso interno, sem custo adicional; recursos disponíveis na unidade.

Erros comuns – evite

- ✕ Ações vagas (“melhorar a fiscalização”) sem dizer o que será feito.
- ✕ Responsável indicado apenas como “a Secretaria”.
- ✕ Prazos indefinidos (“em breve”, “durante o contrato”).
- ✕ Plano aprovado e esquecido, sem juntada ao SEI nem comunicação aos responsáveis.

Antes de avançar, confirme

- ✓ Todo risco não aceito tem ações, correlação lógica, responsáveis, prazos e recursos.
- ✓ Os riscos aceitos têm justificativa.
- ✓ O plano foi validado pelo gestor máximo da unidade.
- ✓ O plano foi juntado ao SEI e comunicado aos responsáveis.

10. Informação, comunicação e monitoramento

Em resumo

O que é: o acompanhamento contínuo do plano e a comunicação dos resultados.

Quem participa: o responsável pelo monitoramento definido no plano e, nas contratações, o gestor e os fiscais do contrato.

Resultado esperado: registros periódicos no SEI e o plano atualizado sempre que necessário.

A etapa de **informação e comunicação** consiste em atividades executadas ao longo de todo o processo de gestão de riscos, envolvendo o compartilhamento contínuo e estruturado das informações relativas aos riscos identificados e às medidas adotadas para seu tratamento, junto a todos os atores envolvidos. Essa comunicação deve ser clara, objetiva, pertinente, consistente e tempestiva.

As informações devem estar permanentemente acessíveis às partes interessadas, atualizadas e registradas no **sistema SEI**, com monitoramento periódico – em periodicidade definida no próprio plano – que responda às seguintes questões:

- ✓ O cronograma estabelecido encontra-se em execução conforme planejado?
- ✓ Eventuais atrasos estão sendo devidamente monitorados e os cronogramas ajustados tempestivamente?
- ✓ Todos os recursos previstos encontram-se efetivamente disponibilizados?
- ✓ De que forma estão sendo registrados e documentados os produtos entregues?
- ✓ As informações relativas ao acompanhamento estão atualizadas e devidamente registradas no sistema SEI?
- ✓ Houve surgimento de novos riscos desde o último monitoramento realizado?
- ✓ A alta administração está sendo regularmente informada acerca do andamento dos trabalhos? De que forma se dá essa comunicação?

Revisão do plano

O plano deve ser revisto sempre que surgirem novos riscos, que houver alteração relevante no objeto ou no contexto, ou que o monitoramento indicar ineficácia das ações. Nas contratações, recomenda-se revisá-lo ao menos na assinatura do contrato e em cada prorrogação ou aditivo relevante.

10.1 Passo a passo do monitoramento

1. **Defina no plano** a periodicidade do monitoramento, o responsável e a forma de comunicação à alta administração.
2. **Em cada data prevista**, responda às questões acima, verifique o andamento de cada ação e reavalie os riscos.
3. **Registre no SEI** o resultado, ainda que nada tenha mudado.
4. **Atualize o plano** se surgirem novos riscos, se um risco se materializar ou se uma ação não estiver funcionando.
5. **Comunique** a alta administração na forma definida, com destaque para riscos altos e extremos.

Caso prático – monitoramento

Periodicidade: **trimestral**. Responsável: **gestora do contrato**. Comunicação: relatório trimestral ao Secretário da Saúde, juntado ao processo no SEI.

No primeiro trimestre, o relatório registrou: portaria de designação publicada e capacitação concluída (R4); conta-depósito vinculada aberta (R1); duas ocorrências de posto descoberto, ambas glosadas (R3); e um **novo risco** – atraso no fornecimento de materiais de limpeza –, que foi incluído no plano.

Erros comuns – evite

- ✕ Monitorar apenas quando surge um problema.
- ✕ Não registrar o monitoramento no SEI.
- ✕ Manter o plano inalterado mesmo após mudanças relevantes no contrato.

PARTE II

Gerenciamento de riscos nas contratações públicas

A Parte II aplica a metodologia da Parte I às contratações regidas pela Lei nº 14.133/2021. As escalas, fórmulas, níveis de risco e o apetite a risco são os mesmos; o que muda é o momento em que a análise é feita, os documentos em que é registrada e os instrumentos específicos previstos na lei, como a matriz de alocação de riscos.

11. A gestão de riscos na Lei nº 14.133/2021

Em resumo

O que é: a aplicação da metodologia às contratações da Lei nº 14.133/2021.

Quem participa: equipe de planejamento da contratação, área demandante, área técnica, agente de contratação, gestor e fiscais.

Resultado esperado: a análise de riscos juntada ao processo na fase preparatória e acompanhada durante a execução.

11.1 Obrigatoriedade

A Lei nº 14.133/2021 tratou a gestão de riscos como elemento estruturante das contratações públicas, em diferentes níveis:

Dispositivo	Comando	Consequência prática
Art. 11, parágrafo único	A alta administração deve implementar processos e estruturas, inclusive de gestão de riscos e controles internos, para avaliar, direcionar e monitorar as licitações e os contratos.	A gestão de riscos é responsabilidade institucional, não apenas da equipe de cada processo.
Art. 18, X	A fase preparatória deve abordar “a análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual”.	Toda licitação deve conter análise de riscos, registrada no processo.
Art. 72, I	A contratação direta é instruída com documento de formalização de demanda e, se for o caso, estudo técnico preliminar, análise de riscos, termo de referência, projeto básico ou executivo.	Nas dispensas e inexigibilidades, a análise de riscos deve ser feita quando a complexidade ou o vulto o exigirem; recomenda-se registrar a justificativa quando não for elaborada.
Art. 22	O edital poderá contemplar matriz de alocação de riscos; ela é obrigatória em obras e serviços de grande vulto e nos regimes de contratação integrada e semi-integrada (§3º).	Ver Capítulo 13.
Art. 169	As contratações devem submeter-se a práticas contínuas e permanentes de gestão de riscos e de controle preventivo.	Os riscos devem ser monitorados durante toda a execução do contrato, não apenas no planejamento.

11.2 Quando e por quem a análise é feita

A análise de riscos da contratação é elaborada na **fase preparatória**, em conjunto com o estudo técnico preliminar (ETP) e o termo de referência ou projeto básico, pela equipe de planejamento da contratação, com a participação da área demandante e da área técnica. Ela deve ser concluída antes da publicação do edital ou da autorização da contratação direta, porque seus resultados podem alterar o próprio desenho da contratação – por exemplo, exigências de qualificação, garantias, forma de pagamento, critérios de medição e cláusulas contratuais.

Quadro 18 – Responsabilidades ao longo da contratação

Agente	Responsabilidade
Equipe de planejamento / área demandante	Identifica, analisa e avalia os riscos; propõe o tratamento; elabora o plano de gerenciamento de riscos e, quando cabível, a matriz de alocação.
Autoridade competente / gestor máximo da unidade	Valida o plano de tratamento quanto à viabilidade econômica e operacional; decide sobre a aceitação de riscos médios.
Agente de contratação e comissão	Considera os riscos relativos à fase de seleção do fornecedor e comunica novos riscos identificados no certame.
Gestor e fiscais do contrato	Executam as ações de tratamento atribuídas à fase de execução, monitoram os riscos e registram as ocorrências no SEI.
Assessoria jurídica e controle interno da unidade (2ª linha)	Orientam e revisam a análise de riscos e a matriz de alocação.
Auditoria-Geral do Município (3ª linha)	Avalia, de forma independente, a adequação e a eficácia da gestão de riscos das contratações.

11.3 Onde registrar

Recomenda-se que o resultado seja formalizado no documento padronizado **“Gestão de Riscos” (AG-9503)** do Sistema de Controle Interno – Licitações e Contratos, juntado ao processo no SEI na fase preparatória. O documento deve conter, no mínimo: identificação da contratação; riscos identificados; análise e avaliação (risco inerente e residual); plano de tratamento; matriz de alocação, quando houver; forma de monitoramento; e assinaturas de quem elaborou e de quem validou (ver Anexo I).

> **Integração com o ETP e o termo de referência**
> Os riscos identificados devem dialogar com os demais documentos do planejamento. Um risco de estimativa de quantidades, por exemplo, é tratado com memória de cálculo no ETP; um risco de inexecução, com garantia, sanções e critérios de medição no termo de referência; um risco de desequilíbrio, com cláusula de reajuste e com a matriz de alocação. A análise de riscos que não se reflete em nenhum desses documentos tende a ser apenas formal.

11.4 A gestão de riscos ao longo da contratação

A análise de riscos não é um documento isolado: ela acompanha a contratação do início ao fim. O quadro a seguir mostra o que fazer em cada momento.

Gestão de riscos em cada momento da contratação

Momento	O que fazer com os riscos
Documento de formalização da demanda	Registrar riscos já percebidos pela área demandante e informações sobre problemas em contratações anteriores.
Estudo técnico preliminar	Realizar a análise de riscos completa (etapas 2 a 6 deste guia) e usar os resultados para escolher a melhor solução.
Termo de referência, projeto e edital	Incorporar os tratamentos: exigências de qualificação, garantias, seguros, instrumento de medição de resultado, critérios de medição, sanções e, quando cabível, a matriz de alocação de riscos.
Seleção do fornecedor	Registrar riscos novos percebidos no certame (impugnações, propostas no limite da exequibilidade).
Assinatura do contrato	Revisar o plano, entregá-lo ao gestor e aos fiscais e confirmar as ações previstas para o início da execução.
Execução	Monitorar na periodicidade definida, aplicar os planos de contingência e registrar tudo no SEI.
Prorrogações e aditivos	Reavaliar os riscos e atualizar o plano.
Encerramento	Registrar as lições aprendidas para a próxima contratação do mesmo objeto.

12. Riscos típicos por fase da contratação

Os riscos de uma contratação podem ser organizados nas três fases do processo. O Quadro 19 reúne exemplos frequentes, que servem de ponto de partida – cada contratação deve ter seus riscos identificados conforme suas particularidades. A ferramenta eletrônica (Capítulo 14) traz uma biblioteca com esses e outros riscos, com causas, controles e ações sugeridos.

Quadro 19 – Exemplos de riscos por fase

Fase	Exemplos de eventos de risco	Controles e tratamentos usuais
Planejamento da contratação	Especificação imprecisa do objeto. Quantidades superdimensionadas ou subdimensionadas. Pesquisa de preços inadequada (sobrepreço ou valor inexequível). Insuficiência de dotação orçamentária. Atraso na conclusão da fase preparatória.	Revisão técnica do TR por servidor distinto do elaborador. Memória de cálculo com série histórica. Cesta de preços com fontes do art. 23 e análise crítica. Verificação prévia do plano de contratações anual e da dotação. Cronograma da fase preparatória.
Seleção do fornecedor	Restrição indevida à competitividade. Conluio entre licitantes. Licitação deserta ou fracassada. Aceitação de proposta inexequível. Conflito de interesses de agente público.	Justificativa técnica de cada exigência; parecer jurídico. Consulta a vínculos societários e a cadastros de sanções (CEIS/CNEP). Revisão do preço estimado e ampliação da divulgação. Diligência de exequibilidade (art. 59). Declaração de inexistência de conflito de interesses (arts. 9º e 14).
Gestão do contrato	Fiscalização deficiente. Atraso ou inexecução pela contratada. Pagamento sem comprovação da execução. Desequilíbrio econômico-financeiro. Aditivos acima dos limites legais (art. 125). Inadimplemento trabalhista em serviços com dedicação exclusiva de mão de obra (art. 121).	Designação formal e capacitação dos fiscais; roteiro de fiscalização. Acompanhamento do cronograma e aplicação tempestiva de sanções. Ateste vinculado a relatório de fiscalização. Cláusula de reajuste e matriz de alocação. Controle de acréscimos e supressões acumulados. Medidas do art. 121, §3º (conta-depósito vinculada, pagamento condicionado à comprovação).

Em **obras e serviços de engenharia**, merecem atenção especial: projeto básico deficiente, orçamento sem referência a sistemas oficiais (art. 23, §2º), ausência de licenças e desapropriações, condições geotécnicas imprevistas, medições indevidas e “jogo de planilha”. Em **serviços contínuos com dedicação exclusiva de mão de obra**, destacam-se: erros na planilha de custos, postos descobertos, repactuação sem comprovação (art. 135), pessoalidade na gestão dos terceirizados e verbas rescisórias não pagas.

Dica

Use a biblioteca como ponto de partida, não como resposta pronta. Ao aproveitar um risco típico, adapte a frase ao seu caso, revise a causa e confira se ele realmente se aplica. Uma lista copiada sem adaptação não cumpre a finalidade do art. 18, X.

13. Mapa de riscos e matriz de alocação de riscos

Em resumo

O que é: a definição, no edital e no contrato, de quem arca com as consequências de cada evento futuro que possa afetar o equilíbrio econômico-financeiro.

Quem participa: equipe de planejamento, área técnica e assessoria jurídica.

Resultado esperado: a cláusula de matriz de alocação de riscos, quando obrigatória ou recomendável.

A Lei nº 14.133/2021 utiliza dois instrumentos distintos, que não devem ser confundidos:

Quadro 20 – Mapa de riscos × matriz de alocação de riscos

Aspecto	Mapa de riscos (gerenciamento)	Matriz de alocação de riscos
Natureza	Instrumento de gestão interna da Administração.	Cláusula contratual (art. 6º, XXVII).
Fundamento	Art. 18, X, e art. 169.	Arts. 6º, XXVII, 22 e 103.
Obrigatoriedade	Em toda licitação; nas contratações diretas, quando cabível (art. 72, I).	Obras e serviços de grande vulto e regimes de contratação integrada e semi-integrada; facultativa nos demais casos.
Pergunta que responde	Quais riscos podem comprometer a contratação e como serão tratados?	Quem arca com as consequências de cada evento superveniente?
Produto	Plano de gerenciamento de riscos (Partes I e II deste guia).	Cláusula do edital e do contrato.

13.1 Conteúdo mínimo da matriz

Nos termos do art. 6º, XXVII, a matriz de riscos deve conter, no mínimo:

a) listagem de possíveis eventos supervenientes à assinatura do contrato que possam causar impacto em seu equilíbrio econômico-financeiro e previsão de eventual necessidade de termo aditivo por ocasião de sua ocorrência;

b) no caso de obrigações de resultado, as frações do objeto em que haverá liberdade para o contratado inovar em soluções metodológicas ou tecnológicas em relação ao anteprojeto ou ao projeto básico;

c) no caso de obrigações de meio, as frações do objeto em que não haverá essa liberdade, devendo haver aderência entre a execução e a solução predefinida, consideradas as características do regime de execução.

13.2 Quando é obrigatória

O edital **obrigatoriamente** contemplará matriz de alocação de riscos quando a contratação se referir a obras e serviços de **grande vulto** ou forem adotados os regimes de **contratação integrada ou semi-integrada** (art. 22, §3º). Nos demais casos, a matriz é facultativa, mas recomendável quando houver riscos relevantes de execução cuja repartição precise ficar clara no contrato.

Valor de grande vulto

Consideram-se de grande vulto as obras, serviços e fornecimentos cujo valor estimado supera o limite do art. 6º, XXII, atualizado anualmente por decreto. Para 2026, o limite é de **R$ 261.968.421,04** (Decreto federal nº 12.807/2025). Confira sempre o decreto vigente no exercício.

13.3 Critérios de alocação

A alocação de riscos deve observar as seguintes regras:

Regra	Fundamento
A matriz deve promover a alocação eficiente dos riscos de cada contrato e estabelecer a responsabilidade de cada parte, bem como os mecanismos que afastem a ocorrência do sinistro e mitiguem seus efeitos.	Art. 22, §1º
A alocação considera a natureza do risco, o beneficiário das prestações e a capacidade de cada parte para melhor gerenciá-lo.	Art. 103, §1º
Os riscos que tenham cobertura oferecida por seguradoras serão preferencialmente transferidos ao contratado.	Art. 103, §2º
A alocação deve ser quantificada para fins de projeção dos reflexos de seus custos no valor estimado da contratação; o valor estimado pode considerar taxa de risco compatível com os riscos atribuídos ao contratado.	Art. 103, §3º; art. 22, caput
Nas contratações integradas e semi-integradas, os riscos associados à escolha da solução de projeto básico pelo contratado são de sua responsabilidade.	Art. 22, §4º
A matriz define o equilíbrio econômico-financeiro inicial do contrato e deve ser observada na solução de pleitos das partes.	Art. 103, §4º
Atendidas as condições do contrato e da matriz, considera-se mantido o equilíbrio econômico-financeiro, renunciando as partes a pedidos de restabelecimento relativos aos riscos assumidos, salvo alterações unilaterais da Administração e aumento ou redução, por legislação superveniente, dos tributos pagos pelo contratado.	Art. 103, §5º
O reequilíbrio por força maior, caso fortuito, fato do príncipe ou fatos imprevisíveis deve respeitar, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.	Art. 124, II, “d”

13.4 Reflexos obrigatórios no contrato

O contrato deverá refletir a alocação realizada pela matriz, especialmente quanto (art. 22, §2º):

- **I –** às hipóteses de alteração para o restabelecimento da equação econômico-financeira nos casos em que o sinistro seja considerado na matriz como causa de desequilíbrio não suportada pela parte que pretenda o restabelecimento;
- **II –** à possibilidade de resolução quando o sinistro majorar excessivamente ou impedir a continuidade da execução contratual;
- **III –** à contratação de seguros obrigatórios previamente definidos no contrato, integrado o custo de contratação ao preço ofertado.

13.5 Modelo de matriz

Quadro 21 – Modelo de matriz de alocação de riscos

Nº	Evento superveniente	Parte responsável	Mecanismo de mitigação	Efeito sobre o equilíbrio	Seguro / garantia
R1	Chuvas acima da média histórica que paralisem a obra.	Compartilhado	Previsão de dias improdutivos no cronograma; registro em diário de obra.	Prorrogação de prazo sem reequilíbrio financeiro, conforme cláusula.	—
R2	Acidente de trabalho no canteiro.	Contratada	Fiscalização das normas de segurança (NR-18).	Não enseja reequilíbrio (art. 103, §5º).	Seguro de responsabilidade civil.
R3	Alteração do projeto por interesse da Administração.	Contratante	Análise técnica prévia das alterações.	Enseja restabelecimento do equilíbrio (art. 130).	—

Exemplo ilustrativo. A alocação deve ser definida caso a caso, segundo os critérios do art. 103.

13.6 Passo a passo da matriz

1. **Verifique a obrigatoriedade:** grande vulto ou contratação integrada/semi-integrada? Se não, avalie se a matriz é recomendável.
2. **Liste os eventos supervenientes** relevantes – em geral, os riscos da fase de execução identificados no Capítulo 5 que afetam custos ou prazos.
3. **Aloque cada evento** à parte com maior capacidade de gerenciá-lo (art. 103, §1º), transferindo ao contratado os riscos seguráveis (art. 103, §2º).
4. **Defina os efeitos:** se o evento enseja ou não reequilíbrio, prorrogação ou resolução, e quais seguros são exigidos.
5. **Quantifique**, quando possível, o reflexo da alocação no valor estimado (art. 103, §3º).
6. **Leve a matriz ao edital e ao contrato** e submeta-a à assessoria jurídica.

Caso prático – é preciso matriz?

A contratação de limpeza **não é de grande vulto** e o regime é **empreitada por preço global**; portanto, a matriz é **facultativa**. A equipe decidiu incluí-la para deixar claros três pontos:

Evento	Parte	Efeito
Aumento salarial por nova convenção coletiva	Contratante	Repactuação, na forma do art. 135, mediante demonstração analítica.
Greve dos empregados da contratada	Contratada	Não enseja reequilíbrio; aplicam-se as sanções por inexecução.
Acidente de trabalho com empregado da contratada	Contratada	Não enseja reequilíbrio (art. 103, §5º); exigência de seguro.

Erros comuns – evite

- ✕ Confundir a matriz de alocação (cláusula contratual) com o mapa de riscos (gestão interna).
- ✕ Alocar à contratada riscos que ela não tem como gerenciar, o que encarece as propostas.
- ✕ Incluir a matriz no edital sem refleti-la nas cláusulas do contrato (art. 22, §2º).

14. Ferramenta de apoio: Assistente de matriz de riscos

Para facilitar a aplicação deste guia, a Auditoria-Geral do Município disponibiliza o **Assistente de matriz de riscos** em **auditoriageral.com.br**, na seção “Ferramentas Práticas”. A ferramenta conduz o usuário pelas etapas do guia, aplica automaticamente as escalas e fórmulas, destaca as pendências de preenchimento e emite o documento “Gestão de Riscos” (AG-9503) em PDF, além de planilha em Excel.

Quadro 22 – Correspondência entre a ferramenta e o guia

Etapa da ferramenta	O que é feito	Capítulos
1. Contratação	Dados do processo e critérios de priorização.	4 e 11
2. Identificação	Eventos, categorias, causas (fonte + vulnerabilidade) e consequências; biblioteca de riscos típicos.	5 e 12
3. Risco inerente	Probabilidade × impacto e mapa de calor.	6
4. Controles	Avaliação dos controles existentes e risco residual.	7
5. Tratamento	Resposta ao risco conforme o apetite a risco e plano de tratamento.	8 e 9
6. Alocação	Matriz de alocação de riscos (obrigatória ou facultativa).	13
7. Monitoramento	Periodicidade, responsável, comunicação e registro no SEI.	10
8. Revisão e emissão	Pendências, assinaturas e emissão do PDF e da planilha.	11.3 e Anexo I

> Os dados digitados ficam apenas no navegador do usuário e no arquivo que ele salvar; nenhuma informação é enviada a servidores. O arquivo de trabalho pode ser reaberto para revisões periódicas do plano.

15. Perguntas frequentes

Quantos riscos devo identificar?

Não há número mínimo ou máximo. Como referência prática, uma contratação comum costuma ter entre cinco e quinze riscos relevantes. Mais importante que a quantidade é que os riscos sejam específicos do objeto e que os principais não fiquem de fora.

Qual a diferença entre risco e problema?

Risco é um evento futuro e incerto; problema é algo que já está ocorrendo. Problemas atuais devem ser resolvidos pela gestão; o que se registra como risco é a possibilidade de que voltem a ocorrer.

Posso usar notas intermediárias, como 3 ou 6?

Não. A escala usa apenas 1, 2, 5, 8 e 10. Os intervalos crescentes destacam os riscos mais relevantes.

Um controle que ainda será implantado reduz o risco residual?

Não. Na etapa de controle (Capítulo 7) consideram-se apenas os controles que já funcionam. Medidas futuras entram no plano de tratamento.

Toda contratação direta precisa de análise de riscos?

O art. 72, I, exige a análise de riscos “se for o caso”. Recomenda-se elaborá-la sempre que a complexidade, o valor ou o histórico do objeto o justifiquem, e registrar a justificativa quando ela não for feita.

Quem assina o documento?

Quem elaborou a análise (“Elaborado por”) e o gestor máximo da unidade, que valida o plano de tratamento (“Validado por”).

O que fazer se um risco se materializar?

Acionar o plano de contingência, registrar a ocorrência no SEI, comunicar a alta administração quando o risco for alto ou extremo e revisar o plano de gerenciamento de riscos.

Preciso refazer a análise a cada prorrogação?

Não é preciso começar do zero, mas o plano deve ser revisto em cada prorrogação ou aditivo relevante, considerando o que ocorreu na execução.

A matriz de alocação substitui a análise de riscos?

Não. A análise de riscos (mapa de riscos) é obrigatória em toda licitação; a matriz de alocação é uma cláusula contratual, obrigatória apenas em alguns casos. Os dois instrumentos se complementam.

Posso usar a ferramenta eletrônica em vez de preencher as tabelas?

Sim. O Assistente de matriz de riscos aplica exatamente a metodologia deste guia e emite o documento padronizado “Gestão de Riscos” (AG-9503).

Conclusão

Implementar uma gestão estruturada e sistemática dos riscos contribui significativamente para o fortalecimento institucional, melhora a eficiência operacional e protege o Município contra adversidades administrativas e financeiras. Nas contratações públicas, a análise de riscos bem feita na fase preparatória reduz aditivos, litígios, paralisações e apontamentos dos órgãos de controle, e aumenta a chance de a contratação alcançar o resultado pretendido.

A adoção rigorosa deste guia assegurará que o gerenciamento dos riscos se torne parte integrante da cultura organizacional do Município.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO Guia 73**: gestão de riscos – vocabulário. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: gestão de riscos – diretrizes. Rio de Janeiro: ABNT, 2018.

BRASIL. Controladoria-Geral da União. **Manual de orientações técnicas da atividade de auditoria interna governamental do Poder Executivo Federal**. Brasília: CGU, 2017.

BRASIL. Controladoria-Geral da União. **Metodologia de gestão de riscos**. Brasília: CGU, 2018.

BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. **Diário Oficial da União**: Brasília, DF, 23 nov. 2017.

BRASIL. Decreto nº 12.807, de 29 de dezembro de 2025. Atualiza os valores estabelecidos na Lei nº 14.133, de 1º de abril de 2021. **Diário Oficial da União**: Brasília, DF, 31 dez. 2025.

BRASIL. Lei nº 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos. **Diário Oficial da União**: Brasília, DF, 1 abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 26 out. 2026.

BRASIL. Ministério do Planejamento, Orçamento e Gestão; Controladoria-Geral da União. Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. **Diário Oficial da União**: Brasília, DF, 11 maio 2016.

BRASIL. Ministério do Planejamento e Orçamento. **Guia metodológico para gestão de riscos**. Brasília: MPO, 2024. Disponível em: https://www.gov.br/planejamento. Acesso em: 26 out. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 31073**: risk management – vocabulary. Geneva: ISO, 2022.

THE INSTITUTE OF INTERNAL AUDITORS. **Modelo das três linhas do IIA 2020**: uma atualização das três linhas de defesa. Lake Mary: IIA, 2020.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Licitações & contratos**: orientações e jurisprudência do TCU. Brasília: TCU, [2024]. Disponível em: https://licitacoesecontratos.tcu.gov.br. Acesso em: 26 out. 2026.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Referencial básico de gestão de riscos**. Brasília: TCU, Secretaria-Geral de Controle Externo, 2018.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Roteiro de auditoria de gestão de riscos**. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2017.

TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO. **Lei nº 14.133/2021 comentada**. São Paulo: TCESP, [2024]. Disponível em: https://www.tce.sp.gov.br/legislacao-comentada/lei-14133-1o-abril-2021. Acesso em: 26 out. 2026.

Anexo I – Estrutura do documento “Gestão de Riscos” (AG-9503)

Estrutura mínima recomendada para o plano de gerenciamento de riscos de uma contratação, a ser juntado ao processo no SEI:

Seção	Conteúdo
1. Identificação da contratação	Secretaria, unidade administrativa, processo SEI, objeto, tipo de objeto, forma de contratação, regime de execução, valor estimado, enquadramento como grande vulto e critérios de priorização atendidos.
2. Metodologia	Referência a este guia, às escalas, às fórmulas, aos níveis de risco e ao apetite a risco.
3. Identificação dos riscos	Nº, evento, categoria, fase, causas e consequências.
4. Análise e avaliação	Probabilidade, impacto, risco inerente, controles existentes, risco de controle e risco residual; mapa de calor.
5. Plano de tratamento	Resposta, ações, correlação lógica, contingência, responsáveis, prazos, metas e recursos.
6. Matriz de alocação de riscos	Quando obrigatória ou adotada: parte responsável, efeito sobre o equilíbrio e seguros ou garantias.
7. Monitoramento	Periodicidade, responsável, forma de comunicação à alta administração e local de registro.
8. Aprovação	Local, data e assinaturas: “Elaborado por” e “Validado por”.

Anexo II – Quadro-resumo

Elemento	Regra
Risco inerente	RI = Probabilidade × Impacto (notas 1, 2, 5, 8 e 10).
Risco residual	RR = RI × Risco de controle (Inexistente 1,00 · Fraco 0,80 · Mediano 0,60 · Satisfatório 0,40 · Forte 0,20).
Níveis de risco	Baixo até 9 · Médio acima de 9 até 39 · Alto acima de 39 até 79 · Extremo a partir de 80.
Apetite a risco	Baixo: pode ser aceito · Médio: aceito com justificativa · Alto e Extremo: tratamento obrigatório.
Descrição do risco	Devido a [causa], poderá ocorrer [evento], o que levaria a [consequência].
Causa	Fonte (pessoas, processos, sistemas, tecnologia, eventos externos, governança, planejamento) + vulnerabilidade.
Respostas	Aceitar · Mitigar · Transferir ou compartilhar · Evitar.
Plano de tratamento	Ações e correlação lógica · Responsáveis · Prazos e metas · Recursos.
Contratações	Análise de riscos obrigatória na fase preparatória (art. 18, X); matriz de alocação obrigatória em grande vulto e contratação integrada/semi-integrada (art. 22, §3º).
Registro	Documento “Gestão de Riscos” (AG-9503) juntado ao processo no SEI e monitorado periodicamente.