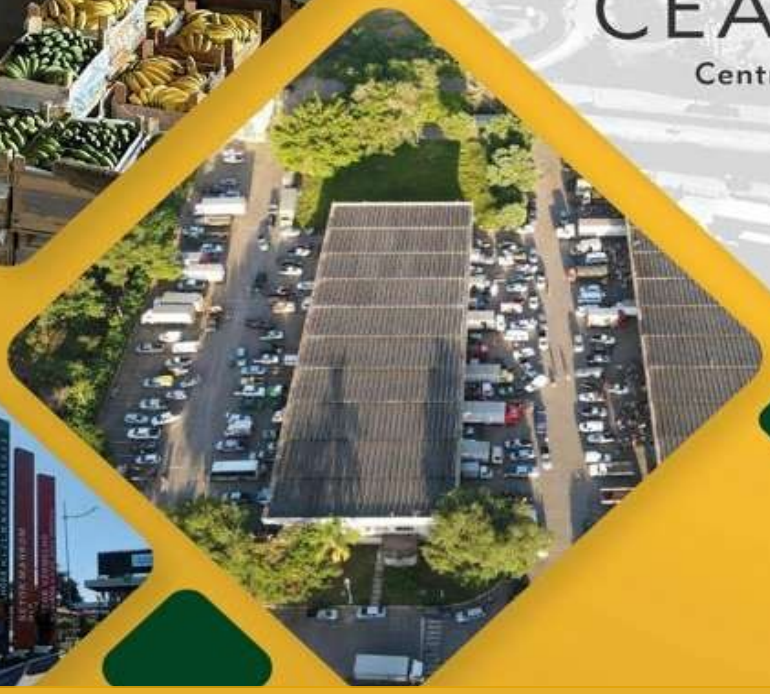






CEASAMINAS
Centrais de Abastecimento

MANUAL DE GERENCIAMENTO DE RISCO DA CEASAMINAS

Contagem 2026

ELABORAÇÃO

CONFORMIDADE E GERENCIAMENTO DE RISCO

Gestor de Conformidade e Gerenciamento de Risco

Luciano Ferreira Ribeiro

APROVAÇÃO

Aprovado pelo COAUD – Comitê de Auditoria Estatuário - na 152ª Reunião Ordinária realizada no dia 10/03/2026.

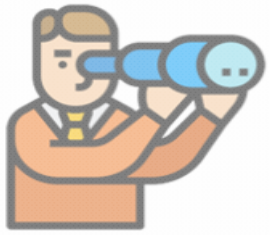
Aprovado pelo CONSAD – Conselho de Administração – na 343ª Reunião Ordinária realizada no dia 20/03/2026.

Contagem, 23 de março de 2026



Missão.

Promover o abastecimento sustentável de alimentos de maneira eficiente e diversificada, gerando desenvolvimento econômico e social para o fortalecimento do sistema agroalimentar".



Visão

"Ser referência em eficiência, inovação e práticas sustentáveis na gestão de centrais de abastecimento alimentar".



Valores

Eficiência; Integridade; Transparência;
Responsabilidade socioambiental;
Foco no cliente; Compromisso; Inovação; Ética.

Sumário

1. INTRODUÇÃO 5

2. CONCEITOS 6

2.1. O QUE SÃO RISCOS? 6

2.2. O QUE É GESTÃO DE RISCOS? 6

2.3. POR QUE FAZER GESTÃO DE RISCOS? 7

2.4. QUAIS SÃO OS OBJETIVOS DA GESTÃO DE RISCOS? 7

2.5. OBJETIVOS DA GESTÃO DE RISCO DA CEASAMINAS. 7

2.6. POLÍTICA DE RISCO DA CEASAMINAS 8

3. METODOLOGIA DE GERENCIAMENTO DE RISCOS 10

3.1. 1ª ETAPA: AMBIENTE DE CONTROLE 10

3.2. 2ª ETAPA: FIXAÇÃO DE OBJETIVOS 11

3.3. 3ª ETAPA: IDENTIFICAÇÃO DE EVENTOS DE RISCOS. 11

3.4. 4ª ETAPA: ANÁLISE E AVALIÇÃO DE RISCO 17

3.5. 5ª ETAPA: RESPOSTA A RISCO 21

3.6. 6ª ETAPA: TRATAMENTO 22

3.7. 7ª ETAPA: INFORMAÇÃO E COMUNICAÇÃO 24

3.8. 8ª ETAPA: MONITORAMENTO 24

4. DIRETIRIZES DA POLITICA DE GESTÃO DE RISCOS DA CEASAMINAS 26

5. COMPETÊNCIAS E RESPONSABILIDADES 28

5.1. Compete ao CONSAD dentro da Gestão de Riscos 28

5.2. Compete ao COAUD dentro da Gestão de Riscos 29

5.3. Compete à Diretoria Executiva dentro da Gestão de Riscos 29

5.4. O objetivo da AUDIN na Gestão de Riscos 30

5.5. Compete ao Comitê de Gestão de Riscos da CEASAMINAS. 31

5.6. Compete aos Gestores de cada processo da CEASAMINAS dentro da Gestão de Riscos 31

6. GLOSSÁRIO 33

7. BIBLIOGRAFIA 37

1. INTRODUÇÃO

O presente Manual de Gerenciamento de Riscos tem como objetivo principal fornecer orientações claras e práticas para a implementação da gestão de riscos na Centrais de Abastecimento de Minas Gerais S/A – CEASAMINAS.

Importante diferenciarmos a termologia de “Gestão de Risco” e “Gerenciamento de Risco”. Vejamos a definição dada pelo TCU:

> Em termos gerais, “**gestão de riscos**” refere-se à arquitetura (princípios, estrutura e processo) para gerenciar riscos eficazmente, enquanto “**gerenciar riscos**” refere-se à aplicação dessa arquitetura para o gerenciamento dos riscos nos diversos contextos específicos em que os objetivos de uma organização são perseguidos (TCU, 2018).
>
> A **gestão de riscos** compreende todas as atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. Não é uma atividade autônoma, separada das demais, mas sim parte de todos os processos organizacionais, incluindo o planejamento estratégico, os projetos e processos de gestão em todos os níveis da organização (TCU, 2018).
>
> Enquanto que **Gerenciamento de riscos** representa as atividades realizadas pelas pessoas em todos os níveis da organização, desde a definição da estratégia até as atividades operacionais, aplicando os princípios, a estrutura e o processo de gestão de riscos para dar suporte à tomada de decisões e à implementação de ações para manter os riscos dentro do nível de apetite e das tolerâncias a riscos estabelecidos pela administração, proporcionando, assim, segurança razoável do cumprimento dos objetivos da organização (TCU, 2018).

O Manual de Gerenciamento de Riscos visa fornecer instrumentos para que os gestores iniciem sua caminhada na gestão dos riscos dos objetos sob sua responsabilidade, além de permitir que a CEAMINAS gradativamente desenvolva sua maturidade à gestão de risco.

Este manual alinha-se à Política de Gestão de Riscos da CEASAMINAS e busca traduzir seus princípios, objetivos e diretrizes em um conjunto de procedimentos e ferramentas, apresenta os fundamentos, o processo e a metodologia de gerenciamento de riscos a ser aplicada com o objetivo de alcançar os objetivos estratégicos.

2. CONCEITOS

2.1. O QUE SÃO RISCOS?



Possibilidade de que ***eventos*** *venham a ocorrer e* ***afetem o alcance da estratégia e dos objetivos do negócio.***

~ COSO ERM 2017

"Tomar consciência dos prováveis riscos e implementar ações para geri-los pode, além de evitar a materialização do risco, contribuir para o processo de tomada de decisão e auxiliar no alcance dos objetivos estabelecidos pela organização." ***~STF 2019***

2.2. O QUE É GESTÃO DE RISCOS?

"Existem duas maneiras de lidar com riscos:

1. ***ser surpreendido*** *por eventos que podem impactar adversamente o alcance dos objetivos da organização e então* ***reagir a eles****, o que caracteriza a cultura de* ***"apagar incêndios";***

2. ***ou antecipar-se a eles****, adotando medidas conscientes que mantenham ou reduzam a probabilidade ou o impacto dos eventos nos objetivos.*

Apenas a segunda maneira pode ser chamada de gestão de riscos*, que também habilita a organização a aproveitar oportunidades".*

~ TCU 2017



A gestão de riscos pode ser definida como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

2.3. POR QUE FAZER GESTÃO DE RISCOS?

O risco é inerente a praticamente todas as atividades humanas, conviver com ele faz parte do cotidiano, mas nem sempre conseguimos percebê-lo. Essa desatenção pode fazer com que seja necessário enfrentar situações difíceis e problemas que, muitas vezes, poderiam ser evitados.

O risco não está presente somente na vida humana, ele está presente também no mundo corporativo. Nas atividades cotidianas das organizações envolve incertezas que podem trazer perdas ou oportunidades. A gestão de risco ajuda a identificar, avaliar e controlar essas incertezas para reduzir impactos negativos e potencializar resultados positivos.

Quando uma organização decide fazer gestão de riscos, ela não elimina as incertezas, mas transforma o inesperado em algo mais previsível e controlado, permitindo a empresa alcançar seus objetivos estratégicos.

2.4. QUAIS SÃO OS OBJETIVOS DA GESTÃO DE RISCOS?

O objetivo da Gestão de Risco é lidar com a incerteza de forma estruturada, protegendo a organização contra perdas e permitindo aproveitar as oportunidades. É proteger os objetivos estratégicos garantindo que a organização consiga cumprir sua missão e visão, mesmo diante dos imprevistos.

2.5. OBJETIVOS DA GESTÃO DE RISCO DA CEASAMINAS.

Os objetivos são os seguintes:

I. **Assegurar que os responsáveis pela tomada de decisão**, em todos os níveis da CEASAMINAS, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso; estabelecendo níveis de exposição a riscos adequados;

II. **Aumentar a probabilidade de alcance dos objetivos da empresa**, reduzindo os riscos a níveis aceitáveis; com estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à estatal;

III. **Agregar valor à organização** por meio da melhoria dos processos de

tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização;

IV. **Proporcionar à CEASAMINAS um perfil mais preventivo e proativo**, possibilitando a antecipação da ocorrência de eventos de riscos nos seus processos de trabalho;

V. **Minimizar incertezas e maximizar oportunidades**, possibilitando que a CEASAMINAS volte sua atenção para ações em áreas/processos mais relevantes.

2.6. POLÍTICA DE RISCO DA CEASAMINAS

A política de risco da CEASAMINAS está baseada na obra de 2004 do COSO ERM[1] que divulgou o trabalho "***Gerenciamento de Riscos Corporativos – Estrutura Integrada***", com foco mais voltado para gerenciamento de riscos corporativos, que definiu gerenciamento de riscos corporativos da seguinte forma:

> ***"É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos."***

Este modelo integra a **gestão de riscos ao planejamento estratégico** de uma empresa, focando na aplicação dos princípios da estrutura para identificar, avaliar e monitorar riscos de forma estratégica e alinhada com os objetivos de desempenho e a cultura organizacional. A estrutura ajuda as empresas a definir seu apetite ao risco, analisar alternativas estratégicas, e estabelecer objetivos de negócios que se alinham com a **missão e a visão**, permitindo a tomada de decisões mais assertivas.

Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

[1] COSO ERM refere-se à estrutura de Enterprise Risk Management (Gestão de Riscos Corporativos) desenvolvida pelo COSO (Comitê das Organizações Patrocinadoras da Comissão Treadway), que oferece um modelo integrado para que as organizações identifiquem, avaliem, respondam e monitorem riscos, alinhando a gestão de riscos à estratégia e ao desempenho geral da empresa. O modelo atualizado de 2017 integra a gestão de riscos com a estratégia e o desempenho, focando na governança, cultura, alinhamento estratégico e nos objetivos das organizações.

a) **Estratégicos:** metas gerais, alinhadas com sua missão;

b) **Operações:** utilização eficaz e eficiente dos recursos;

c) **Comunicação:** confiabilidade de relatórios;

d) **Conformidade:** cumprimento de leis e regulamentos aplicáveis.

O COSO ERM definiu 08 (oito) componentes em sua estrutura, dos quais a CEASAMINAS balizará em sua Gestão de Riscos:

1. **Ambiente de Controle:** este componente está relacionado ao núcleo de qualquer organização, o pessoal (Recursos Humanos) – atributos individuais.

2. **Fixação de Objetivos:** deve ser definido pela Alta Administração e devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite de riscos.

3. **Identificação de Eventos:** processo de identificação de situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização. Podem ser positivos (oportunidades) ou negativos (risco).

4. **Avaliação de Riscos:** visa promover o entendimento do nível do risco e de sua natureza, especialmente quanto à estimativa da probabilidade de ocorrência e do impacto destes eventos. Risco = Probabilidade X Impacto.

5. **Resposta a Risco:** para cada risco identificado, será prevista uma resposta, que pode ser de 4 tipos: **evitar, aceitar, compartilhar *ou* reduzir**.

6. **Atividades de Controle:** geralmente estão expressas em políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos.

7. **Informações e comunicações:** abrangem informações e sistemas de comunicação, permitindo que os colaboradores da CEASAMINAS coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações.

8. **Monitoramento:** compreende o acompanhamento, ao longo do tempo, da qualidade do controle interno, visando assegurar a sua adequação aos recursos e aos riscos.

3. METODOLOGIA DE GERENCIAMENTO DE RISCOS

A Metodologia de Gestão de Riscos objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na CEASAMINAS, por meio da definição de um processo de gerenciamento de riscos.

As etapas de gerenciamento de risco estão baseadas nos 08(oito) componentes definidos pelo COSO ERM.

3.1. 1ª ETAPA: AMBIENTE DE CONTROLE

O ambiente de controle está relacionado ao núcleo de qualquer organização, o pessoal (Recursos Humanos) – atributos individuais e o ambiente organizacional que elas trabalham. É o conjunto de atitudes, valores, políticas e práticas que influenciam a forma como os trabalhadores entendem e executam o controle interno e a gestão de riscos.

O Ambiente de Controle está intrinsicamente ligado aos controles não operacionais, que estão fortemente relacionados com os valores das pessoas da organização e são igualmente importantes para gerar um ambiente de controle saudável.

Ele reflete a cultura ética, a integridade e as "*atitudes e ações do Conselho e da Administração em relação à importância dos controles dentro da organização, definindo o tom da organização",* segundo o Instituto de Auditores Internos (IIA).

O ambiente de controle é a **primeira etapa** do processo de gestão de riscos e serve como fundamento para todas as demais etapas (identificação, avaliação, resposta e monitoramento dos riscos). Sem um bom ambiente de controle, os outros componentes do sistema de gestão de riscos perdem eficácia.

🎯 Objetivo da Etapa

Nesta etapa a CEASAMINAS deve garantir que o ambiente organizacional **apoie e fortaleça** a gestão de riscos, de modo que:

- Haja **responsabilidade** e **transparência**;
- Os controles sejam **respeitados**;
- Os riscos sejam **identificados, avaliados e tratados** de forma consistente.

3.2. 2ª ETAPA: FIXAÇÃO DE OBJETIVOS

Nesta etapa a alta administração deverá definir o apetite a risco da CEASAMINAS que deverá estar alinhado ao objetivo estratégico visando cumprir sua missão e visão. Esta definição é importante pois definirá o limite ou tolerância ao risco que a CEASAMINAS está disposta a aceitar para alcançar seus objetivos. E também garante que a gestão de riscos esteja alinhada com o planejamento estratégico.

O apetite a risco não é fixo, podendo ser revisto periodicamente e conforme a necessidade identificada nas análises de eficácia dos procedimentos de gerenciamento dos riscos.

Em termos práticos, o apetite a risco é o nível de risco que a organização está disposta a aceitar, ou seja, é o limite tolerável de exposição aos riscos identificados, considerando-se o nível de risco atribuído na avaliação, sem que sejam tomadas medidas de tratamento para eliminar, reduzir ou compartilhar.

Definir o apetite ao risco é uma **etapa fundamental** para o sucesso da CEASAMINAS. Ao identificar a quantidade e o tipo de risco que está disposta a assumir, a CEASAMINAS pode tomar decisões informadas, direcionar recursos e implementar medidas de mitigação adequadas, estará melhor preparada para enfrentar os desafios e oportunidades que surgir ao longo do tempo.

🎯 Objetivo da Etapa

Nesta etapa a CEASAMINAS deve, através da alta administração, definir o apetite a risco, ou seja, definir o **nível máximo de risco que pode ser assumido para alcançar seus objetivos**.

3.3. 3ª ETAPA: IDENTIFICAÇÃO DE EVENTOS DE RISCOS.

A etapa de identificação de eventos de risco é uma das mais cruciais do processo, pois consiste em detectar os eventos que podem afetar os objetivos da CEASAMINAS, seja de forma negativa (ameaças) ou positiva (oportunidades). A capacidade de prever e reconhecer riscos antes que eles se manifestem pode ser a diferença entre o sucesso e o fracasso de um projeto ou iniciativa.

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

Nesse sentido, a etapa de identificação dos riscos envolve o reconhecimento, a descrição e o registro dos possíveis eventos de riscos mais relevantes, com a caracterização de suas prováveis causas e possíveis consequências. Nesta fase, identifica-se os eventos de riscos que podem comprometer os resultados e o alcance dos objetivos do processo, projeto, programa, atividade ou iniciativa, objeto da avaliação de riscos, que tenha o potencial de afetar o objetivo estratégico da CEASAMINAS.

Em termos analíticos, o risco deve ser examinado quanto a suas causas e consequências.

RISCO
desvio em relação ao esperado

CAUSAS	CONSEQUÊNCIAS
Fatores que dão origem ao risco, internos ou externos à empresa. São os "gatilhos". Pode ser uma ou muitas	Efeitos negativos resultantes da ocorrência do risco, além do seu impacto sobre o objetivo. Pode ser uma ou muitas

Na identificação dos eventos de riscos devem ser considerados eventos de risco pertencentes às seguintes categorias:



Listamos abaixo alguns exemplos para facilitar o entendimento sobre as categorias de riscos:

RISCOS OPERACIONAL
• Falha no planejamento da ação • Não cumprir o cronograma • Capacidade de execução limitada • Fornecedor de mão de obra ou de insumo
RISCO DE IMAGEM OU REPUTAÇÃO
• Exposição negativa em meios de comunicação • Perda de confiança das partes interessadas
RISCO LEGAL
• Pagamento de multas • Descumprimento de TAC • Descumprimento de legislação especifica
RISCO ORÇAMENTÁRIO/FINANCEIRO
• Desconhecimento de valores de contingências judiciais • Inadimplência dos Concessionários • Falta de liquidez

Para a identificação dos eventos de riscos, sugere-se a realização de **entrevistas** associada ao diagrama de ***Bow Tie***. Esse procedimento dever ser realizado com cada Gestor de Departamento e chefes de seção da CEASAMINAS.

Para que a entrevista tenha maior efetividade procure seguir as orientações:

Planeje a entrevista

Defina a pauta: Utilize uma planilha para a tabulação dos dados coletados;

Identificar os entrevistados e convocá-los com a pauta;

Realização

Procure esclarecer o objetivo da entrevista, caso o entrevistado tenha alguma dúvida;

Faça a descrição do evento de risco respondendo às perguntas:

a. O que pode dar errado? (O que pode acontecer? Que tipo de evento pode impedir o alcance dos objetivos estratégicos? Etc.)
b. Porque o evento pode dar errado? (Porque o evento pode ocorrer? Há falhas em processos, pessoas, sistemas ou infraestrutura que possam gerar este evento de risco? Etc.)

c. Quais seriam as consequências caso o evento ocorra? (Que objetivos ou metas seriam afetados? Etc.)
d. Qual a categoria do risco? (Riscos operacionais; Riscos de imagem/reputação; Riscos legais; Riscos financeiros/orçamentários).

Tabule os dados coletados na planilha;

Cada evento de risco deve ser descrito de forma clara e completa, normalmente contendo:

Elemento	Descrição
Evento de risco	O que pode acontecer (ex.: falha em sistema de TI)
Causa	Por que o evento pode ocorrer (ex.: falta de manutenção do sistema)
Consequência	O que pode resultar (ex.: paralização do sistema)
Categoria do risco	Risco operacional
Departamento Responsável	Área e/ou pessoa que responde pelo Risco (ex.: Departamento de Informatica)

É salutar que, em seguida a identificação ou à elaboração da lista de eventos de risco, sejam identificadas as causas (o que pode originar o risco) e as consequências (o efeito gerado nos objetivos, uma vez concretizado o evento de risco) de cada um dos eventos de risco levantados. Para isso, pode-se usar o diagrama *Bow Tie*.

O que é a análise pelo diagrama de *Bow Tie*?

A análise *Bow Tie* é uma maneira esquemática simples de descrever e analisar os caminhos de um risco desde as causas até as consequências. Pode ser considerada uma combinação do raciocínio de árvore de falhas, que analisa a causa de um evento (representada pelo nó de uma *bow tie*), com árvore de eventos, que analisa as consequências. Entretanto, o foco Bow Tie está nas barreiras entre as causas e o risco, e o risco e as consequências. (MGI, 2024)

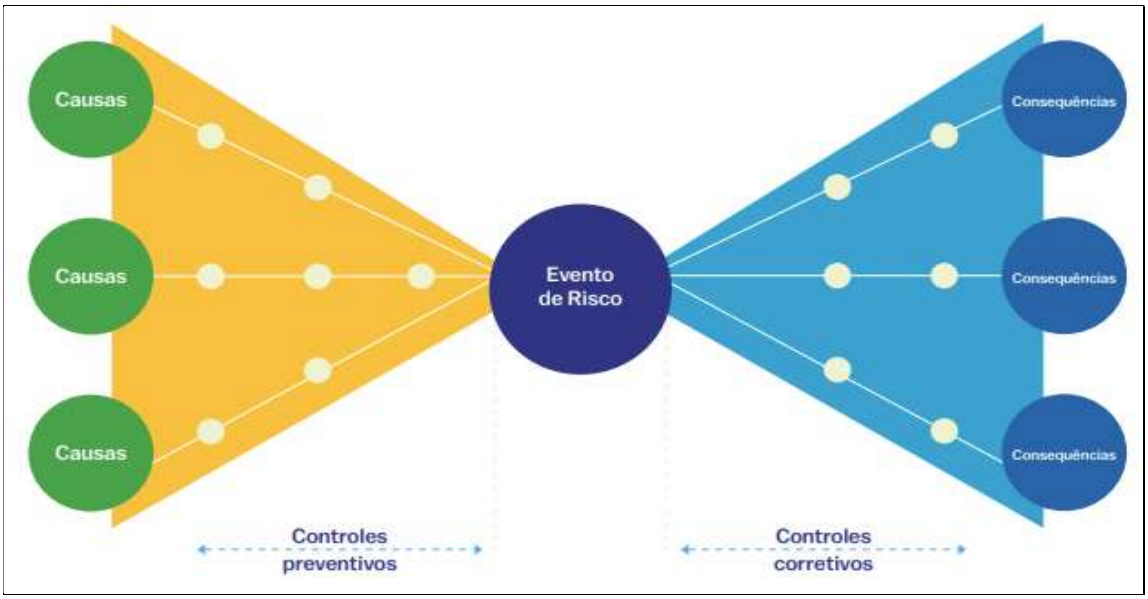


Figura: Diagrama de ***Bow Tie***

Na descrição dos riscos identificados:

- Faça uso da frase contida no quadro abaixo:

> "**Devido a ... (CAUSA/FONTE), poderá acontecer ... (EVENTO DE RISCO), o que poderá levar a ... (EFEITO/ CONSEQUÊNCIAS), impactando no/na ... (OBJETIVO DO OBJETO)".**

Descrever os riscos aplicando o modelo acima ajuda a perceber se, porventura, uma causa, um evento ou uma consequência são partes do mesmo risco.

> **Dica:** Nessa fase é comum perceber que os riscos levantados inicialmente não se tratam de riscos, mas sim causas ou consequências. Uma dica para ser utilizada é: **PESSOAS, SISTEMAS, INFRAESTRUTURA**, geralmente são **CAUSAS de risco**, e não o risco.
> **CAUSA** de risco **FONTE DE RISCO + FRAGILIDADES**

Para facilitar o entendimento, listamos alguns exemplos de causas de riscos mais comuns:

Fator de risco	Fragilidade
Pessoa	Baixa capacitação, desmotivação, corrupção, falta de pessoal, sobrecarga
Processo	Ineficiente, mal estruturado, redundante
Sistema	Obsoleto, incompatível, baixa segurança, não se comunica com outros
Tecnologia	Alto custo, alta complexidade, baixa acessibilidade, ultrapassada

Infraestrutura	Inadequada, precária, insuficiência orçamentária
Evento externo	Influências políticas, crises econômicas, desastres ambientais

Modelo de diagramação do ***Bie Tie*** em planilha de Excel.

CAUSA (fontes / vulnerabilidades) **(Por que o evento pode ocorrer?)**	**EVENTO** (incidente / irregularidade) **(O que pode acontecer?)**	**CONSEQUÊNCIA** (impacto em um objetivo) (Quais as consequências caso o evento ocorra?)

Identificação dos eventos de risco é a **terceira etapa** e é uma das etapas mais importantes, pois o evento de risco é uma situação ou ocorrência incerta que, se acontecer, pode prejudicar ou favorecer os objetivos estratégicos da empresa.

🎯 Objetivo da Etapa

Detectar e descrever quais eventos podem afetar o alcance dos objetivos estratégicos da CEASAMINAS, sejam eles negativos (ameaças) ou positivos (oportunidades). Essa etapa busca entender o que pode acontecer, porque pode acontecer, e quais seriam as consequências.

Ao final desta etapa, deve-se ter a planilha preenchida contendo a lista dos riscos identificados, contento: Descrição do evento de risco; Causas prováveis; e Consequências possíveis.

Exemplo de Planilha de Mapeamento de Risco

MAPEAMENTO DE EVENTOS DE RISCO					
IDENTIFICAÇÃO DO RISCO					
	(O que pode acontecer?)		(É Risco ou Oportunidade)	(Por que o evento pode ocorrer?)	(O que pode resultar?)
Item	EVENTO DE RISCO	CATEGORIA DO RISCO	EFEITO	CAUSA(S)	CONSEQUÊNCIA(S)
1	Queda de energia elétrica na empresa.	Operacional	É Risco	Falha na rede elétrica externa.	Interrupção das atividades diárias e perda de dados.

3.4. 4ª ETAPA: ANÁLISE E AVALIÇÃO DE RISCO

Nesta etapa, cada um dos riscos levantados na fase de identificação deve ser analisado. Para isso, podem ser procuradas informações históricas a fim de se ter melhor entendimento sobre a possibilidade de sua ocorrência e de se identificar o impacto no objetivo caso o risco se materialize.

Nesta etapa, cada um dos eventos de riscos identificado deve ser classificado de acordo com a escala de probabilidade e impacto apresentada nas tabelas a seguir:

PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	**Improvável** Em casos excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias apontam para essa possibilidade	**1**
Baixa	**Rara** De forma inesperada ou mesmo casual, o evento poderá ocorrer, tendo em vista que as circunstâncias pouco indicam essa possibilidade.	**2**
Média	**Possível** De alguma forma, o evento poderá ocorrer, pois as circunstâncias apontam moderadamente essa possibilidade	**3**
Alta	**Provável** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam de forma inconteste essa possibilidade.	**4**
Muito Alta	**Praticamente certa** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam de forma inconteste essa possibilidade.	**5**

Tabela 01: Escala de Probabilidades CEASAMINAS

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	**Mínimo.** Causa impacto nos objetivos (estratégicos, operacionais, de imagem, reputação, legais de conformidade, financeiros orçamentários).	**1**
Baixo	**Pequeno.** Impacta os objetivos (estratégicos, operacionais, de imagem, reputação, legais de conformidade, financeiros orçamentários).	**2**
Médio	**Moderado** Também causa. Impacto nos objetivos (estratégicos, operacionais, de imagem, reputação, legais de conformidade, financeiros orçamentários), porém recuperável.	**3**
Alto	**Significativo.** Gera impacto nos objetivos (estratégicos, operacionais, de imagem, reputação, legais de conformidade, financeiros orçamentários), de difícil reversão.	**4**
Muito alto	**Catastrófico.** Ocorre impacto nos objetivos (estratégicos, operacionais, de imagem, reputação, legais de conformidade, financeiros orçamentários), de forma irreversível.	**5**

Tabela 02: Escala de Consequências da CEASAMINAS

Ao estabelecer as notas para probabilidade e impacto nessa etapa deve ser levado em conta o **risco sem a consideração de quaisquer medidas (controles) eventualmente existentes** (**risco inerente**). Em outras palavras, deve-se ter em mente a pergunta "O que/quanto ocorreria se não tivéssemos controle algum aplicado sob o risco X"?

Dessa forma é possível obter o **Nível de Risco Inerente (NRI)** de cada risco identificado. O NRI consiste no resultado da multiplicação da Probabilidade (P) pelo Impacto (I) sem considerar a ação dos controles existentes.

Nível de Risco Inerente (NRI) = Probabilidade (P) X Impacto (I)

O Risco Inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos; ou seja, **é o risco "puro ou natura**l" de uma atividade – é aquele que existe apenas por ela acontecer, sem considerar políticas, controles internos ou mecanismos de prevenção.

Uma vez calculado o nível do risco inerente a organização deve avaliar se existem controles capazes de mitigar esses riscos; e, caso existam, qual sua eficácia.

Como passo seguinte, devem ser listados as atividades de controles existentes (exemplo: resoluções de diretoria, normas, regulamentos, procedimentos, protocolos, rotinas de sistemas informatizados etc.) que minimizam o impacto e/ou a probabilidade de o risco de manifestar ou que reduzam suas consequências caso ele ocorra. São os controles que a CEASAMINAS já possui que têm a força de reduzir de algum modo o Risco Inerente.

Após a identificação das atividades de controle, torna-se necessário avaliar a eficácia, eficiência e efetividade dos mesmos no tocante aos objetivos do processo. Deve-se avaliar o nível de execução, a amplitude e a adequação desses controles. Para isso, serão utilizados fatores de avaliação do nível de efetividade dos controles existentes. O modelo abaixo sugere critérios de análise:

Nível de Avaliação dos Controles			
Nível de Eficácia	**Descrição tipo de controle**	**Resultado da eficácia**	**Peso da eficácia**
Inexistente	Não existe controle.	Não há	1,00
Baixa	**Existe controle,** porém não são eficazes o suficiente para reduzir o risco de forma significativa. Não funcionam bem na prática.	Pouco eficaz, risco continua alto	0,80
Media	**Controles parciais:** diminuem a probabilidade ou impacto de um risco, porém não abrangem todas a suas vulnerabilidades.	Reduz parte do risco	0,60
Alta	**Controles satisfatório:** funcionam de forma adequada e eficaz, reduzindo o risco a um nível aceitável.	Reduz risco a nível aceitável	0,40
Muito Alta	**Controles fortes:** oferecem alta eficácia na mitigação dos riscos, sendo robustos, bem estruturados e confiáveis.	Reduz risco a nível mínimo	0,20

O Risco residual é aquele que ainda permanece após a resposta da administração, é o que permanece após a aplicação dos controles e medida de mitigação; ou seja, é o **risco que sobra**, mesmo depois que a organização implementa políticas, procedimentos, treinamentos, etc.

Exemplo:

Imagine uma empresa que armazena produtos inflamáveis.

Risco inerente é o perigo de incêndio (pela natureza da atividade).

Medidas de controle (mitigação) – a empresa instala sensores de fumaça, extintores e faz treinamentos.

Mesmo assim, **ainda existe a possibilidade** de curto-circuito ou falha humana causar o incêndio. Esse é o **risco residual**.

Nesta fase do processo utiliza uma planilha de Excel para realizar o cálculo do Nível de Risco Inerente e Risco Residual.

Exemplo de Planilha de Mapeamento de Risco

MAPEAMENTO DE EVENTOS DE RISCO																		
IDENTIFICAÇÃO DO RISCO						AVALIAÇÃO DO RISCO INERENTE						ANALISE DO CONTROLE		CÁLCULO DO RISCO RESIDUAL					
	(Qual a Fonte de risco que está sendo analisada para identificação do evento de risco?)	(O que pode acontecer?)		(Por que o evento pode ocorrer?)	(O que pode resultar?)	Probabilidade (P) (Qual a chance de o risco se concretizar)		Impacto (I) (Qual a consequência se o risco se concretizar)		Nível de Risco Inerente(P X I)		Há atividade de controle	Eficácia do Controle	Probabilidade (P) (Qual a chance de o risco se concretizar)		Impacto (I) (Qual a consequência se o risco se concretizar)		Nivel de Risco Residual	
Nº	Fonte de Risco	Evento de Risco	Categoria do Risco	Causa(s)	Consequência(s)	Peso	Análise	Peso	Análise	Peso	Classificação	Sim/Não	Nível de Eficácia	Peso	Análise	Peso	Análise	Peso	Classificação

Após realização do cálculo do Nível do Risco Residual, deve-se identificar à qual nível de risco o valor resultante corresponde, podendo o nível de risco encontrado ser:

Pequeno, Moderado, Alto ou Crítico.

Risco Pequeno	Risco Moderado	Risco Alto	Risco Crítico
1-3	4-6	8-12	13-25

Tabela 3: Escalas de Classificação dos Níveis de Risco

A partir da escala de classificação de risco é elaborada a matriz de riscos adotada pela CEASAMINAS, que apresenta a disposição gráfica da classificação dos níveis de riscos, conforme as escalas de probabilidade e impacto, desde o pequeno, ao qual são atribuídos os níveis de 1 a 3, até o crítico, ao qual são atribuídos os níveis de 13 a 25.

A matriz mostra não só o nível de risco, mas também como os riscos em análise estão distribuídos em termos de probabilidade e impacto.

Matriz de Risco

Impacto							
	Muito alto	5	Risco Moderado (5)	Risco Alto (10)	**Risco Crítico (15)**	**Risco Crítico (20)**	**Risco Crítico (25)**
	Alto	4	Risco Moderado (4)	Risco Alto (8)	Risco Alto (12)	**Risco Crítico (16)**	**Risco Crítico (20)**
	Médio	3	Risco Pequeno (3)	Risco Moderado (6)	Risco Alto (9)	Risco Alto (12)	**Risco Crítico (15)**
	Baixo	2	Risco Pequeno (2)	Risco Moderado (4)	Risco Moderado (6)	Risco Alto (8)	Risco Alto (10)
	Muito baixo	1	Risco Pequeno (1)	Risco Pequeno (2)	Risco Pequeno (3)	Risco Moderado (4)	Risco Moderado (5)
			1	2	3	4	5
			Muito baixa	Baixa	Média	Alta	Muito alta
			Probabiliade				

Tabela 4: Matriz de níveis de risco residual da CEASAMINAS

A análise e avaliação de risco é **quarta etapa** e é uma das fases centrais do processo de gestão de riscos corporativos. Ela tem como objetivo compreender a natureza dos riscos identificados, avaliar sua probabilidade e impacto, avaliar se a CEASAMINAS já possui algum controle para os riscos identificados e calcular o risco residual. Em sequência os riscos são comparados com os critérios definidos pela CEASAMINAS – como o **apetite e a tolerância.** E por fim, os riscos acima do limite de tolerância, são priorizados de acordo com sua relevância e com os objetivos estratégicos da CEASAMINAS.

🎯 Objetivo da Etapa

É compreender a natureza, a probabilidade e o impacto dos riscos identificados, para que seja possível priorizá-los e decidir quais precisam de tratamento.

No fim desta etapa, é possível entender **o que pode acontecer, por que, e com que gravidade.**

3.5. 5ª ETAPA: RESPOSTA A RISCO

Nesta etapa, é atribuído a cada risco mapeado, uma resposta pré-definida a partir da classificação do nível de risco residual da etapa anterior, a reposta define qual a postura a ser adotada pela CEASAMINAS diante do risco identificado e avaliado.

No âmbito da CEASAMINAS, existem 4 (quatro) possíveis tipos de respostas quanto aos riscos identificados: **evitar, aceitar, compartilhar ou reduzir**.

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a um nível aceitável	Custo desproporcional, capacidade limitada diante do risco já identificado	**Evitar**	Promover ações que evitem, eliminem ou atenuem rapidamente as causas e/ou efeitos
Risco Alto	Indica que o risco reputado de residual será reduzido a um nível compatível com a tolerância a riscos	Nem todos os riscos podem ser transferidos, como Risco de Imagem, Risco de Reputação.	**Reduzir**	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos.
Risco Moderado	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Reduzir a probabilidade ou o impacto, ou ambos.	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou mesmo compartilhamento de uma parte do risco (seguro, transações de hedge ou terceirização da atividade).
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância ao risco	Verificar a possibilidade de retirar certos controles considerados desnecessários.	**Aceitar**	Conviver com o evento de risco, mantendo práticas e procedimentos existentes.

É importante observar que para cada resposta a risco há uma ação de controle estabelecida.

- "**Evitar**" sugere que atenuem rapidamente as causas e/ou efeitos do risco eliminando sua possibilidade de ocorrência;
- "**Reduzir**" sugere que sejam adotadas medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos;
- "**Compartilhar ou transferir**" sugere que o risco seja transferido ou compartilhado com terceiros;

- “**Aceitar**” sugere não fazer nada, conviver com o risco, de forma consciente, e que sejam mantidas práticas e procedimentos já existentes, considerando a impossibilidade de adoção de novas medidas ou que o custo de trata-lo não compense.

A etapa de resposta a riscos é a fase do processo de gestão de riscos corporativos que a organização define se irá reduzir, transferir, aceitar ou evitar os riscos de forma que fiquem dentro do nível de apetite ao risco estabelecido pela organização.

🎯 Objetivo da Etapa

É saber o que fazer com cada risco classificado na etapa anterior. É transformar os resultados da análise de risco em ações práticas, que permitam: evitar o risco, reduzir os riscos, compartilhar ou transferir o risco, e aceitar o risco.

Selecionar e aplicar estratégicas que permitam controlar os riscos e aproveitar oportunidades, garantindo que os objetivos organizacionais sejam alcançados de maneira segura e eficiente.

3.6. 6ª ETAPA: TRATAMENTO

O tratamento dos riscos é uma etapa fundamental da gestão de riscos e abrange o planejamento e a execução de ações preventivas, mitigadoras ou contingenciais que resultem na diminuição da probabilidade e/ou do impacto dos riscos identificados, caso estes se materializem.

Para definir o tratamento a ser dado, devem-se considerar aspectos como a relação custo-benefício, a viabilidade, a tempestividade e os efeitos colaterais da opção de tratamento escolhida para cada risco.

Após definido o tratamento mais adequado, é preciso elaborar um plano de tratamento para cada risco, no qual estarão previstas as ações a serem implementadas para reduzir a probabilidade e o impacto do risco. A elaboração do plano de tratamento será baseada na técnica o 5W2H.

A elaboração do plano tratamento dos riscos deve seguir os seguintes passos:

- **Identifique o evento de risco.** – Descreva claramente o evento de risco.
- **Identifique a categoria do Risco** – ex. Risco Operacional.
- **Identifique o nível de risco** – ex. Risco Crítico.
- **Informe a resposta ao risco que fora atribuída** – ex. Evitar.
- **O que será feito?** Qual tarefa será realizada.
- **Como será feito?** Qual será o processo para realizar a tarefa.
- **Onde será feito?** Área responsável.
- **Quem?** Quem são as pessoas responsáveis pela tarefa.
- **Quanto custará?** Quais serão os custos para realizar a tarefa.
- **Quando será feito?** Data de início e fim da tarefa.
- **Por que será feito?** A razão de realizar a tarefa.

Dicas práticas!

- Caso possua mais de uma medida de controle para o evento de risco, repita o evento na planilha.
- Insira medida de tratamento possível de ser implementada.
- Cada iniciativa deve ter uma única unidade responsável.
- Busque prazos exequíveis.

Modelo do plano de tratamento dos riscos em formato de planilha:

PLANO DE TRATAMENTO DE CONTROLES (5W2H)											
EVENTO DE RISCO		AVALIAÇÃO DO RISCO		COMO SERÁ FEITO? - *(How)*	O QUE SERÁ FEITO? - *" What? "*	ONDE SERÁ FEITO? - *" Where? "*	POR QUEM SERÁ FEITO? - *" Who? "*	QUANTO CUSTARÁ? - *"How much?"*	QUANDO SERÁ FEITO? - *" When? "*		POR QUE SERÁ FEITO? - *" Why? "*
EVENTO DE RISCO	CATEGORIA	NÍVEL (RR)	RESPOSTA	CONTROLE PROPOSTO / AÇÃO PROPOSTA	CLASSIFICAÇÃO DO CONTROLE	ÁREA / SETOR RESPONSÁVEL	NOME / CARGO RESPONSÁVEL	VALOR	INÍCIO (PREVISÃO)	CONCLUSÃO (PREVISÃO)	OBSERVAÇÕES
			0								
			0								

🎯 Objetivo da Etapa

É definir e implementar medidas para modificar o risco, de modo a reduzir sua probabilidade de ocorrência ou impacto negativo, aumentar oportunidades e garantir que o risco residual fique dentro do apetite de risco da organização.

Etapa de tratamento é a fase do processo que a organização define como, quem, quando e com quais recursos as ações de mitigação serão executadas.

3.7. 7ª ETAPA: INFORMAÇÃO E COMUNICAÇÃO

A etapa de informação e comunicação é uma das fases essenciais do processo de gestão de riscos corporativos. Ela garante que todas as partes interessadas recebam informações relevantes, tempestivas e precisas sobre os riscos e os controles, promovendo uma tomada de decisão eficaz e uma cultura organizacional de transparência e responsabilidade.

A informação e comunicação dos riscos organizacionais é composta de atividades realizadas durante todo o processo de gestão de riscos e consiste no compartilhamento contínuo das informações relativas aos riscos identificados e seus respectivos tratamentos com os diversos atores do processo.

A comunicação deve ser clara, objetiva, pertinente, consistente e tempestiva, para que os riscos e seus tratamentos sejam conhecidos por todos que trabalham com o objeto da gestão de riscos, como gestores de riscos. Deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados, e vice-versa, da CEASAMINAS para o ambiente externo e vice-versa.

As informações precisam estar acessíveis às partes interessadas de modo que os envolvidos tenham clareza de seus papéis e suas responsabilidades, além de uma base sólida para a tomada de decisões.

🎯 Objetivo da Etapa

Assegurar que as informações sobre riscos sejam identificadas, coletadas, processadas e comunicadas de forma adequada, permitindo que gestores, colaboradores e partes extras tomem decisões alinhadas as estratégicas e aos objetivos da CEASAMNINAS.

A etapa de informação e comunicação é essencial para garantir que os dados sobre riscos sejam compartilhados de forma clara e oportuna, permitindo decisões eficazes e a integração de todos no processo de gestão de riscos.

3.8. 8ª ETAPA: MONITORAMENTO

O monitoramento de riscos é a etapa final e continua do processo de gestão de riscos corporativos. Seu objetivo é acompanhar continuamente os riscos identificados, se as

ações de tratamento estão sendo eficazes, verificar mudanças no ambiente interno e externo e garantir a melhoria continua do sistema de gestão de riscos da organização.

A atividade de monitoramento dentro do processo de gestão de riscos da CEASAMINAS consiste na verificação, supervisão e acompanhamento contínuo dos riscos identificados ao longo do tempo.

O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno deverá "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento será realizado por meio de:

- Avaliações continuas;
- Avaliações independentes (por exemplo, auditorias internas e externas).

As avaliações continuas de monitoramento objetivam identificar fragilidades e possibilidades de melhoria. Lembrando que riscos e oportunidades mudam ao longo do tempo e devem ser monitoradas para que a CEASAMINAS possa realizar os ajustes necessários.

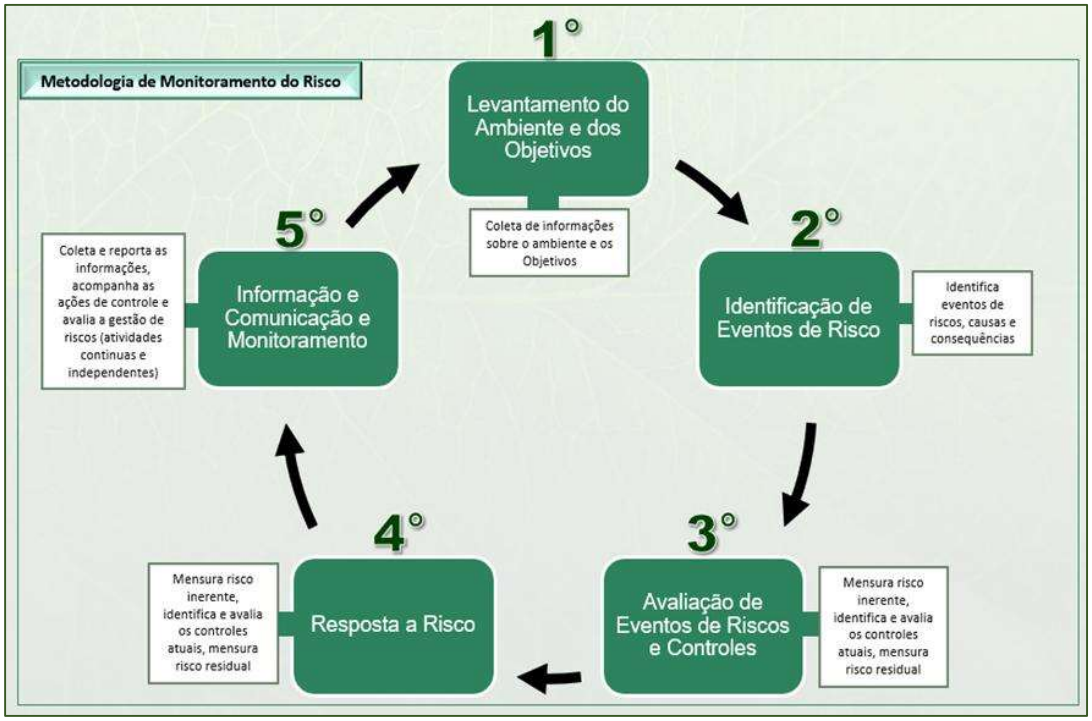
As avaliações continuas, em geral, são operações definidas e rotineiras, fazendo parte das atividades normais da CEASAMINAS, sendo realizadas em tempo real.

As avaliações independentes garantem a eficácia do gerenciamento de riscos ao longo do tempo. Não estão inseridas nas atividades normais do processo, assim podem significar uma visão diferenciada, pois podem ser realizadas por observações, questionários, revisões e outros exames; e podem trazer um feedback sobre o resultado das avaliações continuas.

🎯 Objetivo da Etapa

É assegurar que o processo de gestão de riscos permaneça eficaz ao longo do tempo, identificando mudanças no ambiente interno e externo, e garantindo que todas as partes interessadas estejam informadas sobre a situação dos riscos e das respostas adotadas. É garantir que os riscos sejam reavaliados periodicamente, verificando se as respostas ao risco continuam adequadas e eficaz.

O monitoramento de risco não é uma etapa final e isolada – ele é continuo e cíclico, retroalimentado todas a outras fases (identificação, avaliação, resposta e comunicação).



4. DIRETIRIZES DA POLITICA DE GESTÃO DE RISCOS DA CEASAMINAS

As diretrizes da CEASAMINAS da política de gestão de riscos são:

a) A gestão de riscos **será integrada ao planejamento estratégico**, aos processos e às políticas da CEASAMINAS;

b) Após implementados**, os controles devem ser continuamente avaliados** ao longo do tempo no que diz respeito ao seu desenho e operação;

c) Integração das instâncias de gestão de riscos da CEASAMINAS:

A Gestão de Riscos da CEASAMINAS será baseada em práticas nacionais e internacionais e contém diretrizes que são desenvolvidas no princípio do **Modelo das Três Linhas do IIA 2020.** O modelo das três linhas é uma estrutura de governança e gestão de riscos que ajuda organizações a alcançar objetivos através de três níveis (linhas):

1ª Linha: Gestão Operacional (executa e controla) – Responsável direta por identificar e gerenciar riscos na execução diária das

atividades. Implementa controles internos para atingir os objetivos da organização.

Essa linha é formada pela diretoria e gestores (tomadores de decisão) diretamente envolvidos nas operações do dia a dia da empresa, entregando produtos e/ou serviços aos clientes. Esses profissionais são responsáveis por identificar, avaliar e gerenciar riscos em suas respectivas áreas. Dessa forma, cabe a essa linha implementar controles, políticas e procedimentos que reduzam a probabilidade de falhas a partir do cumprimento de políticas e normas internas, de um controle operacional eficaz, da identificação de riscos e incidentes e da promoção de uma cultura de integridade e conformidade.

2ª Linha: Gestão de Riscos e Compliance (orienta e monitora) – Oferece suporte técnico, monitoramento e supervisão à primeira linha. Ela ajuda a definir as políticas, metodologias e indicadores de risco, sem assumir a propriedade da gestão operacional.

3ª Linha: Auditoria Interna (audita e avalia) – Fornece avaliações independentes e objetivas sobre a eficácia das duas primeiras linhas e da própria governança. Reporta diretamente ao Conselho de Administração e ao Comitê de Auditoria de maneira a manter sua imparcialidade.

Dessa maneira, a terceira linha atua como um observador estratégico, avaliando se os processos, políticas e controles estão sendo aplicados de forma eficaz e se os riscos estão sendo devidamente tratados.

d) Metodologia e ferramentas de apoio à gestão de riscos:

A Gestão de Riscos da CEASAMINAS deve ser sistematizada e suportada pelas premissas da metodologia do ***Committee of Sponsoring Organizations of the Treadway Comission*** – COSO e de boas práticas, com as quais e com as ferramentas de auxílio devem possibilitar a obtenção de informações úteis à tomada de decisão para a consecução dos objetos institucionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos pelas instâncias supervisoras.

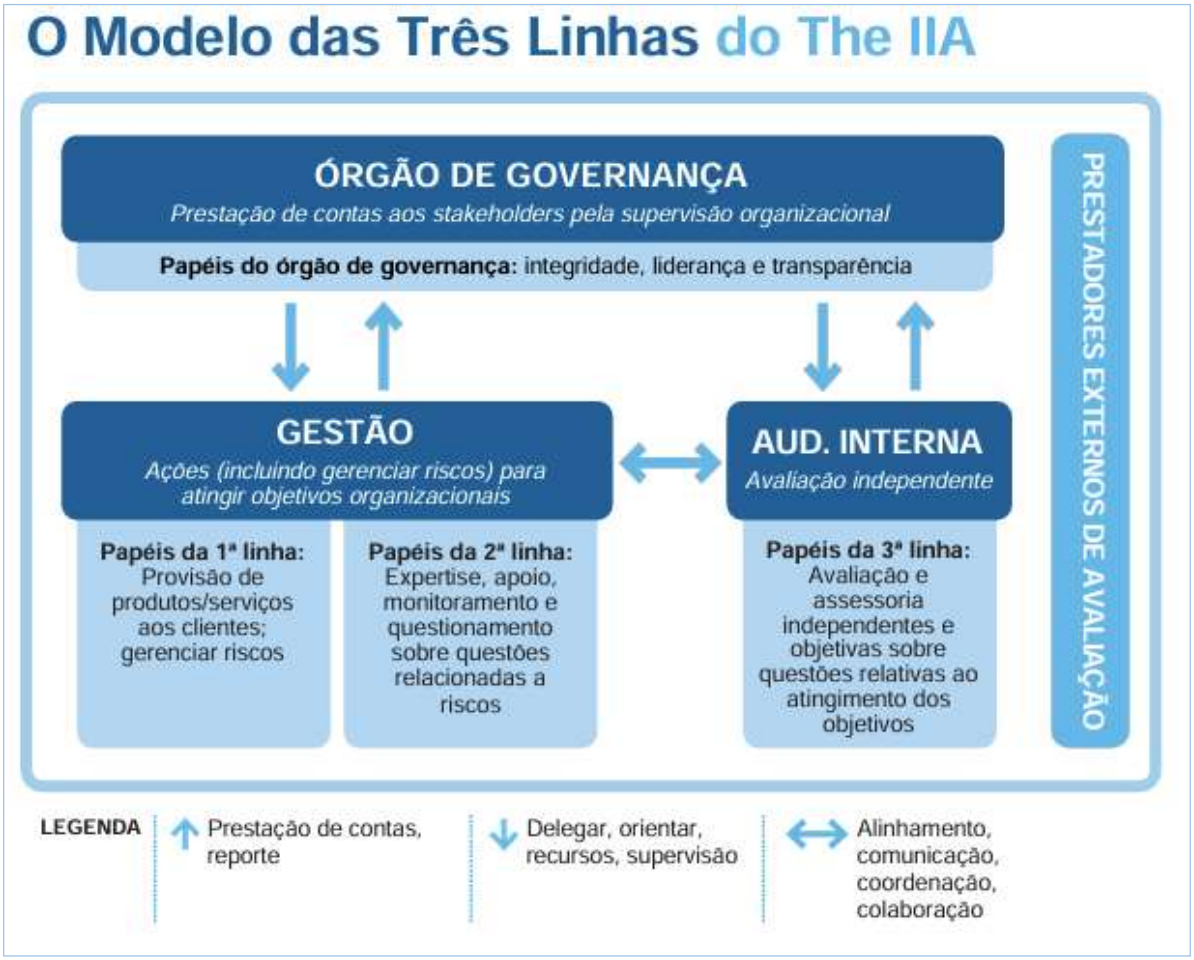


Figura 1 – Representação do Modelo das Três Linhas do IIA 2020

5. COMPETÊNCIAS E RESPONSABILIDADES

As competências e responsabilidades no gerenciamento de riscos são fundamentais para garantir que o processo seja eficaz, transparente e integrado à gestão da organização. Cada área envolvida tem papéis específicos na hierarquia da gestão de riscos. Vejamos:

5.1. Compete ao CONSAD dentro da Gestão de Riscos

I. Aprovar a Política de Gestão de Riscos da Empresa e suas revisões;

II. Definir o nível de exposição ao risco na condução dos negócios da CEASAMINAS;

III. Implementar e supervisionar os sistemas de gestão de riscos, conformidade e controles internos estabelecidos para a prevenção e mitigação dos principais

riscos a que a CEASAMINAS esteja exposta, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e aqueles relacionados a ocorrência de corrupção e fraude; e

IV. Outras atribuições que lhe forem conferidas pela legislação e demais normas aplicáveis.

5.2. Compete ao COAUD dentro da Gestão de Riscos

I. Monitorar a qualidade e a integridade dos mecanismos de controle interno da gestão, das demonstrações financeiras e das informações e medições divulgadas pela Empresa;

II. Avaliar e monitorar a exposição ao risco da CEASAMINAS;

III. Supervisionar as atividades desenvolvidas nas áreas de controle interno, de auditoria interna e de elaboração das demonstrações financeiras da CEASAMINAS; e

IV. Outras atribuições que lhe forem conferidas pela legislação e demais normas aplicáveis, Conselho de Administração, ou pelo Estatuto Social da CEASAMINAS.

5.3. Compete à Diretoria Executiva dentro da Gestão de Riscos

I. Submeter a Política de Gestão de Riscos e suas revisões ao Conselho de Administração da CEASAMINAS;

II. Implementar e assegurar o cumprimento da Política de Gestão de Riscos aprovada pelo Conselho de Administração da CEASAMINAS;

III. Apresentar ao Conselho de Administração, para as medidas cabíveis, proposta dos níveis de exposição a riscos da Empresa, bem como da estratégia de resposta aos mesmos e de melhorias para o sistema de gerenciamento de riscos, conformidade e controles internos;

IV. Aprovar as normas de gerenciamento de riscos, conformidade e controles internos e suas revisões e validar os sistemas de controle de prevenção aos riscos em vigor;

V. Aprovar o portfólio dos riscos da Empresa e os respectivos Planos de Resposta e/ou de Contingência, se aplicável, e submetê-lo ao Conselho de

Administração, promovendo, quando necessário, a revisão e/ou reclassificação dos riscos (classificação atribuída, discordância das avaliações, possíveis macro ações corretivas etc.);

VI. Supervisionar o gerenciamento dos riscos que podem comprometer a execução dos processos e projetos, bem como a realização dos objetivos estratégicos e da prestação de serviços;

VII. Promover a adoção de práticas, princípios de conduta e padrões de comportamento estabelecidos nas diretrizes desta Política;

VIII. Promover a integração e o desenvolvimento contínuo dos colaboradores da CEASAMINAS responsáveis pela governança, gerenciamento de riscos, conformidade e controles internos da Empresa;

IX. Atuar na disseminação da cultura de gerenciamento de riscos, conformidade e controles internos da Empresa; e

X. Outras atribuições que lhe forem conferidas pela legislação e demais normas aplicáveis, Assembleia Geral, Conselho de Administração, ou pelo Estatuto Social da CEASAMINAS.

5.4. O objetivo da AUDIN na Gestão de Riscos

Os art. 6º e 7º do Estatuto da Auditoria Interna da Ceasaminas, instituído através da RD/CONSAD/01/2021 RD/CONSAD/01/2021 de 19.03.2021, estabelece o objetivo da Auditoria Interna, *in verbis*:

> *"Art. 6º. A Auditoria Interna tem por finalidades principais atender ao que dispões o art. 9º § 3º da Lei 13.303/16, bem como prestar apoio aos profissionais da Controladoria-Geral da União e do Tribunal de Contas da União, no exercício do cargo; possuindo, todavia, enfoques e clientes diferentes daqueles dos Controles Interno e Externo.*
>
> *Parágrafo único - A auditoria Interna representa a terceira linha de defesa do sistema de controle interno, que presta serviços de avaliação com base nos pressupostos de autonomia técnica e de objetividade.*
>
> *Art. 7º. A auditoria trabalha com o objetivo de avaliar os resultados alcançados, apresentando recomendações preventivas e corretivas para a melhoria dos processos de governança, do gerenciamento de riscos e dos controles internos da gestão, em caráter preventivo."*

5.5. Compete ao Comitê de Gestão de Riscos da CEASAMINAS.

I. Propor aprimoramentos em políticas, diretrizes e normas complementares para a gestão de riscos ao Conselho de Administração da CEASAMINAS;

II. Assessorar no gerenciamento de riscos dos processos de trabalho priorizados;

III. Acompanhar a implementação das ações e avaliar os resultados;

IV. Monitorar os riscos ao longo do tempo, de modo a permitir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com esta Política;

V. Assegurar que as informações adequadas sobre gestão de riscos estejam disponíveis em todos os níveis;

VI. Disseminar a cultura da gestão de riscos na estatal;

VII. Estimular práticas e princípios de conduta e padrões de comportamento no âmbito de sua atuação;

VIII. Estimular e promover condições à capacitação dos agentes públicos no exercício do cargo, função e emprego em gestão de integridade, riscos e controles internos da gestão;

IX. Fomentar a inovação e a adoção de boas práticas de gestão;

X. Cumprir as recomendações e orientações emitidas pelas Instâncias Superiores sobre Gestão de Riscos;

XI. Promover a implementação de metodologias e instrumentos de gestão de riscos; e

XII. Praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

5.6. Compete aos Gestores de cada processo da CEASAMINAS dentro da Gestão de Riscos

I. Executar e gerenciar os riscos dos processos de negócio e/ou dos projetos sob sua responsabilidade, de acordo com esta Política e as correlacionadas, bem como garantir a implantação do modelo de gerenciamento de riscos,

conformidade e controles internos adotados pela CEASAMINAS;

II. Comunicar ao Comitê de Gestão de Riscos identificados e avaliados e os respectivos Planos de resposta aos Riscos e/ou de Contingência, após a aprovação do Diretor ao qual esteja vinculado, bem como o status das ações previstas nos referidos planos;

III. Atuar na implementação de ações corretivas para resolver deficiências em processos e/ou controles;

IV. Manter controles internos eficazes;

V. Apoiar no monitoramento dos riscos de seus processos e/ou projetos ao longo do tempo, objetivando que as respostas adotadas resultem na manutenção dos riscos em níveis adequados, de acordo com o modelo de gerenciamento de riscos aprovado com esta Política;

VI. Disseminar preceitos de comportamento íntegro e da cultura de gerenciamento de riscos, conformidade e controles internos, junto à sua equipe e em sua área de atuação;

VII. Buscar a inovação e a adoção de boas práticas de governança, de gestão de riscos, conformidade e controles internos;

VIII. Cumprir as recomendações e observar as orientações emitidas pela pelo Comitê de Gestão de Riscos; e

IX. Cumprir a legislação aplicável e normativos internos da empresa.

6. GLOSSÁRIO

Análise de riscos: processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades.

Apetite a risco: quantidade de risco em nível amplo que uma organização está disposta a aceitar na busca de seus objetivos. Quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir (TCU, 2018).

Área de conformidade e gerenciamento de riscos: área responsável por propor políticas de conformidade e gerenciamento de riscos; coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a CEASAMINAS; coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados;

Avaliação de riscos: processo global para estimar a magnitude dos riscos, e decidir se um risco é ou não tolerável, bem como propor formas de mitigação dos riscos constatados.

Compliance: no verbo inglês “to comply”, que quer dizer cumprir, obedecer, estar de acordo, define-se Compliance como seguir as leis, normas e procedimentos internos das organizações, além de parcerias éticas.

Comunicação e consulta: consulta processos contínuos e iterativos que uma empresa conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos.

Consequência: resultado de um evento que afeta determinados objetivos.

Contratadas: empresas contratadas pela CEASAMINAS para prestação de serviços.

Contexto externo: ambiente externo no qual a empresa busca atingir seus objetivos.

Contexto interno: ambiente interno no qual a empresa busca atingir seus objetivos.

Controle interno: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão da Companhia.

Critérios de riscos: termos de referência contra os quais o significado de um risco é avaliado.

Estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a empresa.

Evento: ocorrência ou alteração em um conjunto específico de circunstâncias nos contextos interno e/ou externo, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo ou positivo.

Fator de risco: elemento que, individualmente ou combinado, possui potencial intrínseco para dar origem ao risco.

Frameworks: é um conjunto de técnicas, ferramentas ou conceitos pré-definidos usados para resolver o problema de um projeto ou domínio específico. É, basicamente, uma estrutura de trabalho que atua com funções pré-estabelecidas que se adaptam à situação e à organização em questão.

Gerenciamento de riscos: é a aplicação da arquitetura implantada internamente na empresa, de modo a identificar, em todos os níveis e unidades da empresa, quais são os eventos capazes de impactar seus objetivos, para então, adotar medidas de tratamento de riscos, mantendo-os em conformidade com o nível definido como tolerável pela empresa.

Gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a empresa, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestores: ocupantes das funções de liderança, tais como gestores de departamento, gerentes de unidades e coordenadores de seção, que tenham equipes sob sua gestão.

Governança: combinação de processos e estruturas implantadas pela alta administração da empresa, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.

Identificação de riscos: processos de busca, reconhecimento e descrição de riscos.

Incerteza: deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua probabilidade, sua consequência ou impacto.

Impacto: efeito resultante da ocorrência do evento.

Medida de Controle: medida aplicada pela empresa para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais sejam alcançados.

Meta: alvo ou propósito com que se define um objetivo a ser alcançado.

Monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

Nível de risco: magnitude de um risco, expressa em termos da combinação das probabilidades e dos impactos dos riscos.

Objetivo Organizacional: situação que se deseja alcançar de forma a evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da empresa;

Oportunidade: Um risco é considerado oportunidade quando tem um impacto positivo, ou seja, quando a ocorrência do risco pode trazer benefícios para a companhia, de forma que possa levar a melhorias nos processos, inovações, aumento da eficiência ou vantagem competitiva.

Política de gestão de riscos – documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos (ABNT, 2009).

Probabilidade: chance de um evento acontecer.

Processo: é um conjunto de atividades com uma ordenação específica, com uma ou mais entradas, que cria saída de valor para o cliente e possui começo e fim claramente identificados, podendo subdividir-se em subprocessos.

Proprietário do Risco – é o responsável direto pela gestão dos Riscos associados às operações da Companhia a qual encontram-se sob sua responsabilidade. É a pessoa e/ou o Gestor que detém o conhecimento operacional e/ou técnico, da área que gerencia, capaz de propor a ação de mitigação do risco.

Risco: possibilidade de ocorrência de um evento que possa ter impacto no cumprimento dos objetivos.

Risco Estratégico: associados a tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da Companhia.

Risco inerente: é o risco a que uma empresa está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou o seu impacto (art. 2.º, XIV, IN Conjunta MP/CGU n.º 01/2016).

Risco residual: é o risco a que uma empresa está exposta após a implementação de ações gerenciais para o tratamento do risco (art. 2.º, XV, IN Conjunta MP/CGU n.º 01/2016).

Tolerância ao risco: limiar de risco a partir do qual certos resultados das operações da empresa podem ser comprometidos. É um indicativo da sensibilidade da empresa em relação aos riscos.

Tratamento de riscos: processo para modificar os riscos.

7. BIBLIOGRAFIA

Brasil. Centrais de Abastecimento de Minas Gerais. Estatuto da Auditoria Interna da Ceasaminas / RD/CONSAD/01/2021. – Contagem: CeasaMinas, 2021. https://www.transparencia.ceasaminas.com.br/upload/rfm/Auditoria/Estatuto_da_Auditoria_Interna/Estatuto_Audin_versaofinal_2020.pdf

Brasil. Centrais de Abastecimento de Minas Gerais. Política de Gestão de Riscos Ceasaminas – Contagem: CeasaMinas, 2020. https://www.transparencia.ceasaminas.com.br/upload/rfm/Gestao de Riscos/Gestao de Riscos CEASAMINAS.pdf

Brasil. Supremo Tribunal Federal (STF). Guia de gestão de riscos [recurso eletrônico] / Supremo Tribunal Federal. – Brasília: STF, Secretaria de Gestão Estratégica, Escritório de Gestão Aplicada, 2019.

Brasil. Tribunal de Contas da União. 10 passos para a boa gestão de riscos / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2018.

Brasil. ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO 31000: Gestão de Riscos: Princípios e diretrizes. Rio de Janeiro, 2009.

Brasil. Tribunal de Contas da União. Roteiro de Avaliação de Maturidade da Gestão de Riscos / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018.

Brasil. Ministério da Gestão e da Inovação em Serviços Públicos. Gestão de Riscos, 1ª Edição, 2024. - Brasília, 2024

THE INSTITUTE OF INTERNAL AUDITORS RESEARCH FOUNDATION (IIARF). Modelo das Três Linhas do IIA 2020: uma atualização das Três Linhas de Defesa. Tradução: Instituto dos Auditores Internos do Brasil IIA Brasil, julho de 2020. Disponível *https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia 2020*

The Committee of Sponsoring Organizations of the Treadway Commission – COSO. Gerenciamento de Riscos Corporativos - Integrado com Estratégia e Performance. COSO, 2017.