POLÍTICA DE GESTÃO DE RISCOS CEASAMINAS

Elaborado pela “Comissão de Gestão de Riscos ”, criada pela RD/CONSAD/02/20, composta pela Sra. Elenice Ferreira Pinheiro Cruz e pelos Srs. Názio Veloso da Silva, Geovan da Silva Pereira, André Luiz de Castro Ferreira e Samuel Pereira Barreto.

CONTAGEM/MG

2020

ÍNDICE

POLÍTICA DE GESTÃO DE RISCOS DA CEASAMINAS

01 - JUSTIFICATIVA

A incerteza ou o risco é inerente a praticamente todas as atividades humanas. No mundo corporativo, onde as empresas estão expostas a uma miríade de incertezas originadas de fatores econômicos, sociais, legais, tecnológicos e operacionais, a gestão de riscos é crucial para que se alcance os objetivos estratégicos.

No ambiente de trabalho, muitas vezes depara-se com fatores internos e externos que tornam incerto o êxito do atingimento dos objetivos dos processos ou das atividades que se encontram em desenvolvimento. Independentemente da área em que se atua, e até na vida pessoal, os riscos (ameaças ou oportunidades) podem afetar o andamento da ação, levando-a a uma direção completamente diferente daquela inicialmente planejada.

Nesse contexto, a Política de Gestão de Riscos da CEASAMINAS torna-se uma importante orientadora para ajudar na tomada de decisões baseadas em metodologias e normas que geram, dentre outros benefícios, a redução ou a eliminação de possíveis eventos que poderiam ameaçar o atingimento dos objetivos, os cumprimentos de prazos, leis e regulamentos etc., e, a implementar estratégia evitando o consumo intenso de recursos para solução de problemas quando esses surgirem inesperadamente, bem como para a melhoria contínua dos processos organizacionais.

02 - OBJETIVOS DA GESTÃO DE RISCOS DA CEASAMINAS

Os objetivos que se pretende alcançar com um programa de Gestão de Riscos 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.

03 - REFERENCIAL TEÓRICO

Embora exista uma grande quantidade de metodologias e estruturas de gestão de riscos mundialmente reconhecidas, tais como ISO 31000, Orange Book, do Tesouro Britânico, esta Política de Gestão de Riscos foi baseada na estrutura do COSO ERM, considerando que é o framework definido pela Portaria nº 426/2016, que aprovou a Política de Gestão de Integridade, Riscos e Controles da gestão do Ministério do Planejamento, Desenvolvimento e Gestão - PIRC.

COSO (*Committee of Sponsoring Organizations)* é o Comitê das Organizações Patrocinadoras, da Comissão Nacional sobre Fraudes em Relatórios Financeiros. Criada em 1985, é uma entidade do setor privado – ou seja, foi uma iniciativa do setor privado, independente –, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros, principalmente para estudar as causas da ocorrência de fraudes em relatórios financeiros. Cabe ressaltar que a origem do modelo COSO está relacionada a um grande número de escândalos financeiros, na década de 70, nos Estados Unidos, que colocaram em dúvida a confiabilidade dos relatórios corporativos.

De acordo com o Comitê, **Controle Interno** é:

> *Um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização*

> *dos objetivos relacionados a operações, divulgação e conformidade*. (COSO, 2013)

Em 2004, o COSO divulgou o trabalho **"Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO ERM)"**, com um foco mais voltado para o 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. (COSO ERM, 2004)*

De acordo com o COSO ERM, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização.

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

> 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 oito componentes em sua estrutura, dos quais a CEASAMINAS balizará em sua Gestão de Riscos: ambiente de Controle; fixação de Objetivos; identificação de Eventos; avaliação de Riscos; resposta a Risco; atividades de Controle; informações e comunicações; e monitoramento.

04 - AMBIENTE DE CONTROLE

Este componente está relacionado ao núcleo de qualquer Organização, o pessoal (Recursos Humanos) – atributos individuais, principalmente integridade, valores éticos e competência, e o ambiente no qual operam. Ele provê uma atmosfera na qual as pessoas conduzem suas atividades

e cumprem suas responsabilidades de controle, servindo de base para os demais componentes, retrata a "*consciência e a cultura de controle*" e é afetado fortemente pelo histórico e cultura da organização.

Segundo o Instituto de Auditores Internos (IIA), o Ambiente de Controle representa "*as atitudes e ações do Conselho e da Administração em relação à importância dos controles dentro da organização, definindo o tom da organização*".

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. Entretanto, não são detectados pelas abordagens e ferramentas tradicionais de identificação e avaliação, requerendo técnicas não tão comumente utilizadas, para que se obtenham evidências suficientes sobre a existência desse componente, tais como a observação do ambiente.

O ambiente de controle deve demonstrar o grau e comprometimento em todos os níveis da administração, com a qualidade do controle interno em seu conjunto. É o principal componente e os fatores relacionados ao ambiente de controle incluem, dentre outros:

- Integridade e valores éticos;

- Competência das pessoas da entidade;

- Estilo operacional da organização;

- Aspectos relacionados com a gestão;

- Forma de atribuição da autoridade e responsabilidade.

05 - FIXAÇÃO DE OBJETIVOS

Definidos pela alta administração, os objetivos devem ser divulgados a todos os agentes que prestam serviços para a CEASAMINAS, antes da identificação dos eventos que possam influenciar na consecução dos objetivos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

06 - IDENTIFICAÇÃO DE EVENTOS

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.

Eventos:

- Negativos (Riscos);

- Positivos (Oportunidades).

Por meio da identificação de eventos, pode-se planejar o tratamento adequado para as oportunidades e para os riscos, que devem ser entendidos como parte de um contexto, e não de forma isolada.

Isso porque, muitas vezes, um risco que parece trazer grande impacto, pode ser minimizado pela existência conjunta de uma oportunidade.

Após a identificação de eventos, por meio da avaliação de riscos, deverá ser determinada qual a forma de tratamento para cada risco identificado, e qual o tipo de resposta a ser dada a esse risco.

No mapeamento e avaliação dos riscos, deverão ser consideradas, entre outras possíveis, as seguintes tipologias de riscos:

a) **riscos operacionais**: eventos que podem comprometer as atividades da empresa, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

b) **riscos de imagem/reputação da CEASAMINAS**: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade da estatal em cumprir sua missão institucional;

c) **riscos legais**: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da empresa; e

d) **riscos financeiros/orçamentários**: eventos que podem comprometer a capacidade da CEASAMINAS de contar com recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução

orçamentária, como atrasos no cronograma de licitações.

07 - AVALIAÇÃO DE RISCO

A organização deve estar consciente dos riscos relevantes que envolvem o negócio, bem como deve gerenciar esses riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Assim, é pré-requisito o estabelecimento, pela CEASAMINAS, de objetivos estratégicos alinhados à sua Missão e Visão, para que ela opere de forma conjunta e organizada.

A gestão de riscos (identificação e avaliação de riscos e definição de respostas, dentre elas controles) interage com o Planejamento Estratégico, na medida em que a CEASAMINAS ao identificar e tratar os riscos e implementar controles internos focados nesses riscos, estará aumentando a probabilidade de alcance dos objetivos definidos, ou seja, a gestão de riscos é considerada uma boa prática de Governança da Organização, ao incluir aspectos relacionados a *accountability* (prestação de contas, no sentido de que a gestão está alinhada às diretrizes estratégicas), Transparência (que é um pré requisito para uma adequada prestação de contas), dentre outros.

08 - ANÁLISE DE RISCOS

A análise de riscos é o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos (ABNT, 2009).

O risco é em função tanto da probabilidade como da medida das consequências. Desse modo, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos:

$$\text{Risco} = \textit{função}\ (\text{Probabilidade e Impacto})$$

O resultado final desse processo será o de atribuir a cada risco identificado uma classificação, tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco, expressas em termos tangíveis ou intangíveis.

Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação dessas, e ser

mais ou menos detalhada (ABNT, 2009). O método e o nível de detalhamento da análise podem ser influenciados pelos objetivos, pela natureza do risco, pela disponibilidade de informações e de recursos.

Métodos qualitativos definem o impacto, a probabilidade e o nível de risco por qualificadores como “alto”, “médio” e “baixo”, com base na percepção das pessoas.

Métodos semiquantitativos usam escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco. A escala pode ser linear, logarítmica ou de outro tipo. As fórmulas também podem variar de acordo com a necessidade e o contexto.

Métodos quantitativos estimam valores para as consequências e suas probabilidades a partir de valores práticos e calculam o nível de risco a partir de unidades específicas definidas no desenvolvimento do contexto.

Observe-se que a análise quantitativa necessita de dados factuais e, devido à falta dessas informações ou ao grau de esforço exigido, poderá não ser sempre possível ou desejável. Nesses casos, de acordo com a norma NBR ISO/IEC 31010, a utilização de um método qualitativo ou semiquantitativo, baseado na opinião de especialistas, pode ser suficiente e eficaz (ABNT, 2012).

Em análises qualitativas e semiquantitativas, considerando que a lógica subjacente seja que o nível de risco é proporcional tanto à probabilidade como ao impacto, a função ‘Risco’ será essencialmente um produto dessas variáveis.

Risco = Probabilidade X Impacto

Em sua forma qualitativa mais elementar, a relação entre os riscos e os seus componentes pode ser ilustrada por meio da matriz que segue.

Ressalte-se que, em situações reais, essas escalas são construídas de modo compatível com o contexto e os objetivos específicos da atividade objeto da gestão de riscos.

Quadro 01: Escala de Probabilidades CEASAMINAS

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 inequívoca, o evento ocorrerá, as circunstâncias apontam claramente essa possibilidade.	**5**

Quadro 02: Escala de Consequências da 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

09 - NÍVEL DE RISCO INERENTE

O nível de risco inerente (NRI) é o nível de risco antes da consideração das respostas que a Administração adota para reduzir a probabilidade do evento ou os seus impactos nos objetivos, incluindo controles internos. Resulta da combinação da probabilidade com o impacto (no nosso exemplo, por meio de multiplicação).

Os riscos resultantes do processo de análise, sejam inerentes ou residuais, deverão de modo consistente estar de acordo com os limites de exposição aceitáveis pela CEASAMINAS.

Quadro 3: Escala de classificação de risco da CEASAMINAS

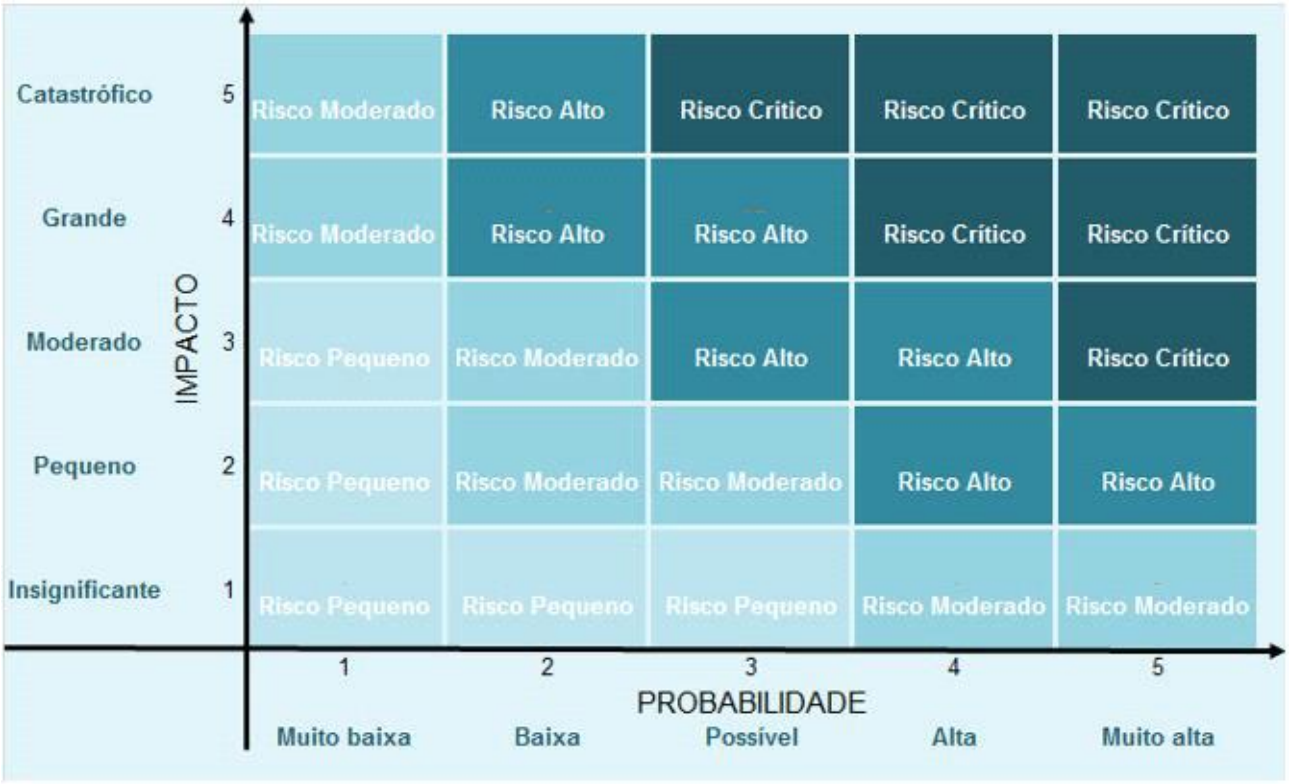


Figura - Cálculo do risco residual

10 - RESPOSTA A RISCOS

Para cada risco identificado, será prevista uma resposta, que pode ser de 4 tipos: **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 a risco	Verificar a possibilidade de retirar certos controles considerados desnecessários.	**Aceitar**	Conviver com o evento de risco, mantendo práticas e procedimentos existentes.

Em relação a riscos é importante apresentar dois conceitos.

i - **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;

ii - **Risco residual** é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes.

De acordo com o COSO, “Evitar” sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. “Reduzir” ou “Compartilhar” reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto “Aceitar” indica que o risco inerente já esteja dentro das tolerâncias ao risco.

É importante observarmos que aceitar o risco é uma forma de responder ao risco. Ou seja, se eu “não fizer nada” em relação ao risco, eu ainda assim estou respondendo a ele, desde que esse “não fizer nada” seja consciente. Isso pode vir a ocorrer quando o custo de implementação de uma medida qualquer para responder a determinado risco fique muito alto, maior até do que os benefícios que a resposta traria para a organização.

11 - ATIVIDADES DE CONTROLE

As Atividades de Controle geralmente estão expressas em políticas e procedimentos de controle, que devem ser estabelecidos e aplicados para auxiliar e assegurar que ações identificadas pela Administração, como necessárias para tratar os riscos relacionados ao cumprimento dos objetivos da Organização, sejam

realizadas de forma eficaz. As atividades de controle estão comumente voltadas para três categorias de riscos: de processo ou operacionais; de registros; e de conformidade. Assim, as atividades de controle deverão contribuir para que:

- *Os objetivos sejam alcançados;*
- *As diretrizes administrativas sejam cumpridas;*
- *As regulamentações externas sejam atendidas;*
- *As ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da CEASAMINAS estejam sendo implementadas.*

As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, deverão vir a prevenir ou administrar os riscos inerentes ou em potencial da CEASAMINAS.

Não são exclusividade de determinada área da CEASAMINAS, sendo realizadas em todos os níveis.

São exemplos de tipologias de atividades de controle:

- *Atribuição de autoridade e limites de alçada;*
- *Revisão de superiores;*
- *Normatização Interna;*
- *Autorizações e Aprovações;*
- *Controles Físicos;*
- *Segregação de Funções;*
- *Capacitação e Treinamento;*
- *Verificações;*
- *Conciliações;*
- *Indicadores de Desempenho;*
- *Programas de Contingência e Planos de Continuidade dos Negócios;*
- *Travas e restrições de sistemas.*

12 - INFORMAÇÃO E COMUNICAÇÃO

Abrangem informações e sistemas de comunicação, permitindo que os colaboradores da CEASAMINAS coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações. Importante que toda a

informação relevante, relacionada aos objetivos – riscos - controles, sejam capturadas e comunicadas por toda a CEASAMINAS.

A CEASAMINAS também deve possuir mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir externamente aquelas que sejam relevantes aos *stakeholders*[1], inclusive à sociedade, que, no caso dessa Sociedade de Economia Mista do Governo Federal, é considerada a principal parte interessada.

A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, econômicos, operacionais e estratégicos. 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.

13 - MONITORAMENTO

Compreende o acompanhamento da qualidade do controle interno, visando assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos. Pressupõe uma atividade desenvolvida 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 contínuas;
- Avaliações independentes (por exemplo, auditorias internas e externas).

A CEASAMINAS deverá utilizar as atividades continuas e independentes, ou uma combinação de ambas, para assegurar que os componentes de controle interno estejam presentes e funcionando.

Diferentemente das Atividades de Controle, que são concebidas para dar cumprimento aos processos e políticas da CEASAMINAS e visam tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de

[1] Os **stakeholders** são pessoas e organizações que podem ser afetadas por um projeto ou empresa, de forma direta ou indireta, positiva ou negativamente. Os **stakeholders** fazem parte da base da gestão de comunicação e são muito importantes para o planejamento e execução de um projeto específico.

melhorias. Lembrando que riscos e oportunidades mudam ao longo do tempo e devem ser monitoradas para que a CEASAMINAS possa realizar os ajustes necessários.

13.1 - Avaliações contínuas

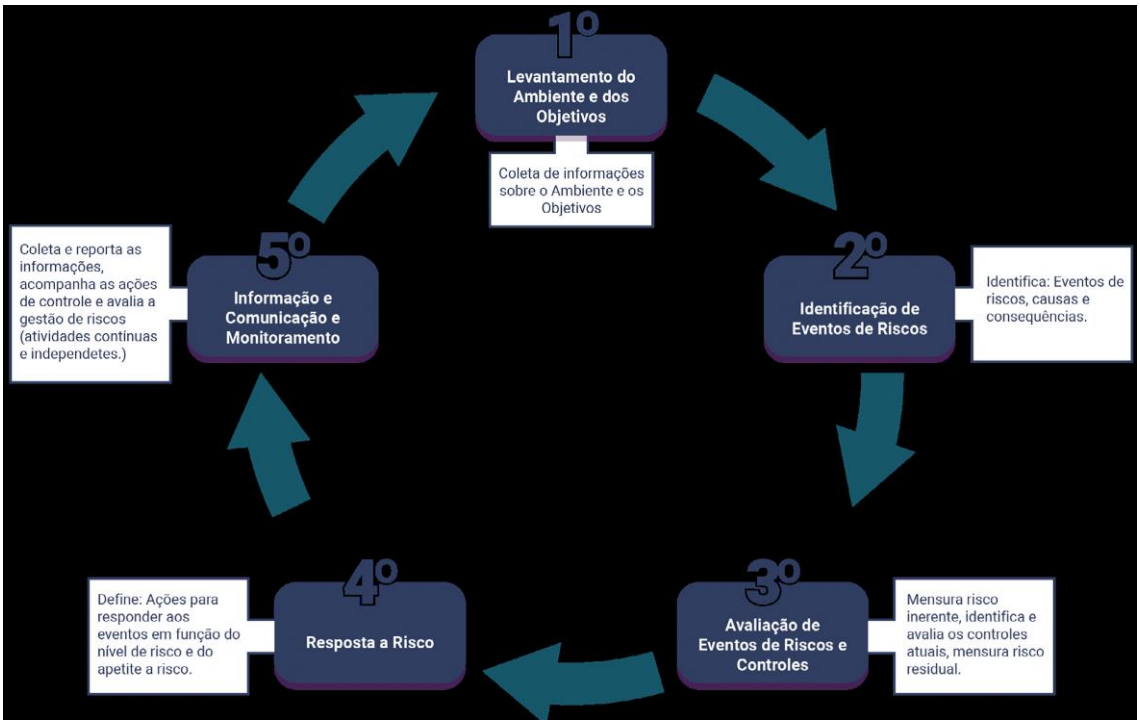
As avaliações contínuas, em geral, são operações definidas e rotineiras, fazendo parte das atividades normais da CEASAMINAS, sendo realizadas em tempo real. Podem ser automatizadas ou manuais, e normalmente são realizadas pelos administradores das áreas responsáveis pelo processo.

Caberá ao gestor do processo definir quais os controles, dependendo da prioridade dos riscos, que deverão ser acompanhados, estabelecendo na rotina do processo a avaliação contínua desses controles.

13.2 - Avaliações Independentes

As avaliações independentes garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Não estão inseridas nas atividades normais do processo, assim podem significar uma visão diferenciada se cada um dos componentes do COSO estão presentes e funcionando.

Podem ser realizadas por observações, questionamentos, revisões e outros exames. Embora os riscos mais prioritários sejam objeto de avaliação contínua ou independente, a avaliação independente pode trazer um feedback sobre o resultado das avaliações contínuas, podendo haver aumento da quantidade de avaliações independentes conforme seja necessário.



14 - DAS DIRETRIZES DA POLÍTICA DE GESTÃO DE RISCOS DA CEASAMINAS

É de vital importância que a empresa possua diretrizes de uma política de gestão de riscos , no caso da CEASAMINAS, são eles:

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, utilizando o conceito das Três Linhas de Defesa, no qual os colaboradores são os donos dos

processos e automaticamente são os proprietários dos riscos.

Os Processos serão conduzidos pelos gestores da CEASAMINAS e respectivos colaboradores, que são os proprietários dos riscos, responsáveis diretos em implementar as medidas preventivas e contingenciais, é a primeira linha de defesa da Gestão de Riscos.

A segunda linha de defesa será da área técnica, a Comissão de Gestão de Riscos que fornece a metodologia, sensibiliza e supervisiona a primeira linha de defesa. Tanto a primeira linha de defesa quanto a segunda linha de defesa se reportarão e se comunicarão com a Diretoria da CEASAMINAS, apresentando relatórios, indicadores e os controles de suas áreas. Deve haver uma forte integração e interação entre as duas linhas de defesa, através do apoio e suporte da Alta Administração da CEASAMINAS para que o processo realmente seja operacionalizado e internalizado em todos os níveis da empresa.

A terceira linha de defesa será a Auditoria Interna, que possui total independência em inspecionar e auditar tanto a segunda linha, verificando a aderência do processo de gestão de riscos e o respectivo controle sobre a primeira linha de defesa, como a operacionalização do processo dessa linha de defesa. A linha de comunicação da terceira linha de defesa será direta com a Diretoria e Conselho de Administração da CEASAMINAS. Desta forma o processo possuirá Governança e será retroalimentativo.

e) 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.

15 - SOLUÇÃO TECNOLÓGICA

A solução tecnológica caracteriza-se como um instrumento de apoio a aplicação da metodologia da Gestão de Riscos. Inicialmente, a solução será disponibilizada em uma planilha dotada das configurações necessárias para aplicação da metodologia. Posteriormente, de forma a garantir uma maior padronização e salvaguarda dos dados, um sistema será disponibilizado e terá os requisitos desejáveis.

A solução tecnológica tem que atender aos seguintes pontos:

- Interface com outros sistemas;
- Classificação de Processos que sejam Críticos;
- Sequência lógica de trabalho – COSO II;
- Matriz de Riscos;
- Elaboração de um Plano de Implementação de Controles;
- Visão integrada de Gestão de Riscos;
- Inventário dos riscos;
- Geração de indicadores de riscos;
- Monitoramento de forma constante e integrado;
- Geração de relatórios, gráficos e estatísticas;
- Gestão dos planos de Implementação de Controles.

O Sotfware público Agatha – Gestão de Riscos, disponibilizado gratuitamente pelo Ministério do Planejamento será a ferramenta utilizada no auxílio a implementação da Gestão de Riscos da CEASAMINAS.

15.1 - O desenvolvimento contínuo dos colaboradores em gestão de riscos;

Capacitação anual dos colaboradores que exercem cargo, função ou atividade em gestão de riscos, deve ser desenvolvida de forma continuada, por meio de soluções educacionais, em todos os níveis.

15.2 - Medição do desempenho da Gestão de Riscos da CEASAMINAS:

A medição do desempenho da gestão de riscos deve ser realizada mediante atividades contínuas ou de avaliações independentes ou a combinação de ambas; o desenvolvimento e implementação de atividades de gestão de riscos

devem considerar a avaliação de mudanças, internas e externas, que contribuam para identificação e avaliação de vulnerabilidades que impactam os objetivos institucionais.

16 - DOS COMPROMISSOS

Por meio desta Política de Gestão de Riscos Corporativos da CEASAMINAS, fica estabelecido os seguintes compromissos:

a) Proporcionar um ambiente saudável e seguro às pessoas, patrimônio e operações;

b) Mitigar os riscos com impactos significativos aos processos, ao meio ambiente, bem como os perigos/riscos no trabalho, atendendo à legislação e outros requisitos subscritos que se relacionem com a operação;

c) Prevenir a poluição do ar, da água e do solo, e destinar adequadamente seus resíduos;

d) Promover a melhoria contínua do desempenho do Processo de Gestão de Riscos;

e) Garantir a interação entre os envolvidos disponibilizando informação por meio de eficazes canais de comunicação, assegurando a consistência e tempestividade das informações que são relevantes para a tomada de decisões;

f) Cumprir as leis e regulamentos locais, nacionais e internacionais, normas e política interna, aplicáveis aos negócios da estatal;

g) Treinar, conscientizar e desenvolver a competência em gestão de riscos e a cultura em controles internos nos empregados;

h) Incentivar a aplicação de tecnologias na melhoria contínua dos aspectos de riscos e seus controles internos nas operações e nas suas instalações;

i) Fornecer condições para que a Comissão de Gestão de Riscos possa contribuir com a CEASAMINAS de

forma a alcançar com sucesso sua missão e atingir sua visão;

j) Disseminar a cultura sobre a importância dos controles internos a todos os empregados e prestadores de serviço;

k) Alinhar a estrutura de controles internos aos riscos e objetivos do negócio;

l) assegurar a existência de atribuição de responsabilidade e de delegação de autoridade, observada a estrutura hierárquica estabelecida pela CEASAMINAS, garantido a apropriada segregação de funções, de modo a eliminar atribuições de responsabilidades conflitantes, assim como reduzir e monitorar, com a devida independência requerida, potenciais conflitos de interesses existentes nas áreas de negócio;

m) Promover a elaboração de relatórios sobre a situação dos controles internos, a serem apreciados e aprovados, no mínimo semestralmente, pelos Comitês competentes e pelo Conselho de Administração da CEASAMINAS.

17 - COMPETÊNCIAS E RESPONSABILIDADES

17.1 - Compete ao Conselho de Administração da CEASAMINAS 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.

17.2 - Compete ao Comitê de Auditoria Estatutária da CEASAMINAS 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.

17.3 - Compete à Diretoria Executiva da CEASAMINAS 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.

17.4 - Compete à Auditoria Interna da CEASAMINAS

I - Atuar no gerenciamento de riscos, conformidade e controles internos da CEASAMINAS, procedendo à avaliação da operacionalização dos controles internos da Empresa, da governança e do processo de gerenciamento de riscos, com foco na melhoria contínua dos processos organizacionais e no aprimoramento dos controles internos;

II - Examinar a adequação e eficácia dos controles internos e das informações contábeis e operacionais da Empresa para evitar fraude, erros, ineficiências e outras irregularidades causadas por agentes internos e externos, contribuindo para minimizar os riscos envolvidos no desempenho das atividades organizacionais;

III - Aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança, e a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações, visando o preparo de demonstrações financeiras;

IV - Apreciar o portfólio dos riscos da Empresa e os respectivos Planos de Resposta e/ou de Contingência, se aplicável, sugerindo, quando necessário, a revisão e/ou reclassificação dos mesmos (classificação atribuída, discordância das avaliações, possíveis macro ações corretivas, etc.); e

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

17.5 - 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.

17.6 - 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 à Comissão de Gestão de Riscos os 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 Comissão de Gestão de Riscos; e

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

18 - REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **Gestão de Riscos: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000**: Primeira Edição, 2009.

BRASIL. Ministério do Planejamento e Controladoria-Geral da União. Instrução Normativa Conjunta Nº 1, de 10 maio de 2016. **Dispõe sobre Controles Internos, Gestão de Riscos e Governança no âmbito do Poder Executivo federal**. Brasília, 2016. Disponível em <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=14&-data=11/05/2016>. Acesso em: novembro de 2020.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **POLÍTICA DE GESTÃO DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS DA GESTÃO DO MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO. Brasília, 2017. Disponível em <**https://repositorio.cgu.gov.br/handle/1/41827>. Acesso em: novembro de 2020.

BRASIL. Ministério da Economia. **Curso Gestão de Riscos nos Processos de Trabalho (Segundo o Coso)**. ENAP, 2018. Online. Realizado em outubro 2020.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Assessoria Especial de Controles Internos – AECI, 2017.

Brasil. Tribunal de Contas da União. **Referencial básico de gestão de riscos / Tribunal de Contas da União**. – Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018.