SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO CENTRO-OESTE

ATO SUDECO Nº 9, DE 18 DE NOVEMBRO DE 2020.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA, RISCOS, CONTROLES E INTEGRIDADE DA SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO CENTRO - OESTE - SUDECO, no uso de suas atribuições que lhe confere a Portaria nº 150, de 17 de maio de 2018, RESOLVE:

Art. 1º Aprovar a Metodologia da Gestão de Riscos e Controles Internos da Superintendência do Desenvolvimento do Centro - Oeste - Sudeco, conforme descrito no Art. 9° da Política de Gestão de Riscos, e no Plano da Gestão de Riscos e Controles Internos da Superintendência do Desenvolvimento do Centro - Oeste - Sudeco na forma do Anexo deste Ato.

Art. 2º Este Ato entra em vigor na data de sua publicação.

NELSON VIEIRA FRAGA FILHO

Presidente do Comitê de Governança, Riscos, Controles e Integridade - CGIRC

ANEXO I

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO CENTRO - OESTE
COMITÊ DE GOVERNANÇA, RISCOS, CONTROLES E INTEGRIDADE

METODOLOGIA DA GESTÃO DE RISCOS E CONTROLES INTERNOS

Superintendência do Desenvolvimento do Centro - Oeste

Superintendente
Diretoria de Administração - DA
Diretoria de Implementação de Programas e Gestão de Fundos – DIPGF
Diretoria de Planejamento e Avaliação - DPA
Auditoria
Ouvidoria
Chefia de Gabinete
Núcleo de Gestão de Riscos e Controle - NGRC

SUDECO
2020

1. PREFÁCIO

Os riscos são inerentes às atividades pessoais, profissionais e institucionais, podendo envolver ameaças ou oportunidades. Eles existem independente da atenção que damos a eles. Nesse sentido, e tendo ciência que todos os processos de trabalho desta Superintendência envolvem riscos, apresentamos esta Metodologia, alinhado com nosso Plano Estratégico, para adotar medidas mitigadoras e de monitoramento para gerenciar as ameaças de modo a mantê-las em níveis aceitáveis.

A Estrutura da Gestão de Governança, Riscos e Controles Internos da Superintendência do Desenvolvimento do Centro-Oeste é composta pela Política de Gestão de Riscos, pelo Plano de Gestão de Riscos e Controles Internos e pela presente Metodologia. Para embasar a elaboração desses documentos, foram utilizados como referencial teórico as normas e regulamentos vigentes destacadas abaixo, dentre outros:

- Instrução Normativa Conjunta n° 1, de 10 de maio de 2016, a qual dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;
- Resolução n° 15, de 16 de outubro de 2017, a qual dispõe sobre a instituição da Política de Gestão de Riscos;
- ABNT NBR ISO 31000:2009;
- Committee of Sponsoring Organizations of the Treadway Commission - COSO (Gerenciamento de Riscos Corporativos - Estrutura Integrada);
- Resolução n° 12, de 13 de setembro de 2017, a qual aprova o regimento Interno do Comitê de Governança, Riscos e Controles da Superintendência do Desenvolvimento do Centro-Oeste – Sudeco; e
- Plano Estratégico 2018 – 2022 da Superintendência do Desenvolvimento do Centro Oeste.

Segundo a NBR 31000:2009 “A gestão de riscos não é uma atividade autônoma separada das principais atividades e processos da organização. A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças”.

Uma boa gestão de riscos busca, dentre outros benefícios, o aumento da probabilidade de alcance dos objetivos planejados, o aprimoramento do processo de identificação de oportunidades e ameaças, o fornecimento de uma base sólida e segura para a tomada de decisão e planejamento, maior eficácia na alocação e no uso de recursos, a melhora na eficiência operacional e na redução das perdas, melhora na conformidade com os requisitos legais e normativos, melhor controle e governança corporativa.

Substanciando o exposto acima, a Gestão de Riscos deverá apoiar de forma decisiva as ações que permitirão à Sudeco cumprir sua missão, visão, propósito e valores consignados no Plano Estratégico.

2. GLOSSÁRIO

Para fins deste documento, consideram-se os seguintes conceitos, extraídos do art. 3º da Resolução n° 15, de 16 de outubro de 2017:

- **Apetite a risco:** nível de risco que a Sudeco está disposta a aceitar;
- **Avaliação de risco:** processo de identificação e análise dos riscos relevantes para o alcance dos objetivos da Sudeco e a determinação de resposta apropriada;
- **Categoria de Riscos**: classificação dos tipos de riscos definidos pela Sudeco que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público. Essas categorias de riscos abrangem riscos estratégicos, operacionais, legais, orçamentários, financeiros, de imagem e reputação, de comunicação e de conformidade.;
- **Causas ou Fatores do Risco**: condições que viabilizam a ocorrência de um evento que impacta os objevos. Resulta da junção das fontes de risco com as vulnerabilidades;
- **Contexto**: diz respeito à definição dos parâmetros externos e internos e dos critérios de risco a serem levados em consideração no gerenciamento de riscos;
- **Consequência:** resultado de um evento que afeta positiva ou negativamente os objetivos da Sudeco;
- **Controle:** qualquer medida aplicada no âmbito da Sudeco, para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados;
- **Controles internos da gestão:** conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão da Sudeco;
- **Escopo**: é a soma dos produtos do processo de trabalho e seus requisitos ou características;
- **Ética:** refere-se aos princípios morais, sendo pré-requisito e suporte para a confiança pública;
- **Fonte de Risco**: elemento (pessoas, processos, sistemas, estrutura organizacional, infraestrutura física, tecnologia, eventos externos) que, individualmente ou de maneira combinada, tem o potencial intrínseco para dar origem ao risco;
- **Fraude:** quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança, que não implicam o uso de ameaça de violência ou de força física;
- **Gerenciamento de risco**: conjunto de processos adotados para identificar, avaliar, administrar, controlar potenciais eventos ou situações e fornecer segurança razoável ao alcance dos objevos organizacionais;
- **Governança:** combinação de processos e estruturas implantadas pela alta administração da Sudeco, para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos;
- **Gestores de Riscos**: são considerados gestores de riscos em seus respectivos âmbitos e escopos de atuação: o superintendente, diretores, chefe de gabinete, coordenadores-gerais, ouvidor, coordenadores, assessores, chefes de divisão, chefes de serviço e os responsáveis pelos processos de trabalho, projetos e ações desenvolvidos;
- **Identificação de riscos:** processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;
- **Impacto:** efeito resultante da ocorrência do evento;
- **Incerteza:** incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;
- **Meta**: alvo ou propósito com que se define um objetivo a ser alcançado;
- **Monitoramento:** componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;
- **Nível de risco:** magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência;

- **Objetivo organizacional**: situação que deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;
- **Órgão de Controle Interno**: unidades administravas, integrantes dos sistemas de controle interno da administração pública federal, incumbidas, entre outras funções, da verificação da consistência e qualidade dos controles internos e da eficácia da gestão de riscos, bem como prestar apoio às atividades de controle externo, exercidas pelo TCU;
- **Política de gestão de riscos:** declaração das intenções e diretrizes gerais da Sudeco relacionadas a gestão de riscos;
- **Processo de gestão de riscos:** aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;
- **Proprietário do risco:** pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;
- **Probabilidade:** possibilidade de ocorrência de um evento;
- **Resposta a risco:** qualquer ação adotada para lidar com risco, podendo ser: aceitar o risco por uma escolha consciente; transferir ou compartilhar o risco a outra parte; evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências;
- **Risco:** possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade;
- **Risco inerente:** risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade dos riscos ou seu impacto;
- **Risco residual:** risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;
- **Tolerância ao risco:** nível de variação aceitável quanto à realização dos objetivos;
- **Tratamento de riscos:** processo de estipular uma resposta aos riscos;
- **Vulnerabilidade:** ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concrezação de um evento indesejado;

3. OBJETIVO

A presente Metodologia visa o cumprimento da Resolução n° 15, de 16 de outubro de 2017, que dispõe sobre a instituição da Política de Gestão de Riscos, e encontra-se em consonância com a Instrução Normativa Conjunta MP/CGU n° 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

De acordo com o art. 5° da Resolução n°15, de 16 de outubro de 2017, a Política de Gestão de Riscos tem por objetivos:

> […]
>
> I - suportar a missão, a continuidade e a sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos;
>
> II - proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica dos processos de trabalho;
>
> III - produzir informações íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas, que proporcione a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica dos processos de trabalho;
>
> IV - assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e as normas internas da Sudeco;
>
> V - salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida;
>
> VI - possibilitar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais a Sudeco está exposta, inclusive para determinar questões relativas à delegação, se for o caso;
>
> VII - aumentar a probabilidade de alcance dos objetivos institucionais, reduzindo os riscos a níveis aceitáveis;
>
> VIII - agregar valor por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização;
>
> IX - estimular a cultura da melhoria contínua dos processos organizacionais, a partir dos resultados gerados pela gestão de riscos e controles internos da gestão no âmbito da Sudeco;
>
> X - orientar os processos de identificação, comunicação, avaliação, classificação, priorização, tratamento e monitoramento dos riscos inerentes às atividades desenvolvidas na Sudeco; e
>
> XI - incorporar a Gestão de Riscos à tomada de decisões em conformidade com as melhores práticas de Governança, por meio do acesso tempestivo a informações suficientes quanto aos riscos aos quais a Sudeco está exposta, bem como ao nível de exposição ao risco suportado.
>
> […]

Ainda de acordo com a Resolução n°15, que trata da Política de Gestão de Riscos, seu art. 6° preceitua:

> […]
>
> II - a atuação da gestão de riscos deve ser dinâmica e formalizada por meio de metodologias, normas, manuais e procedimentos;
>
> III - as metodologias e ferramentas implementadas devem possibilitar a obtenção de informações úteis à tomada de decisão para a consecução dos objetivos institucionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos pelas instâncias supervisoras;
>
> […]

Os princípios norteadores da Governança, Riscos, Controles e Integridade conforme preceitua o art. 4° da Resolução n°15, de 16 de outubro de 2017, são:

> […]
>
> I - aderência aos valores éticos;
>
> II - concepção e proteção de valores institucionais;
>
> III - definição à alta administração do compromisso de atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos institucionais;
>
> IV - definição dos objetivos estratégicos que possibilitam a eficaz gestão de riscos e controles da gestão;
>
> V - gestão sistemática, estruturada, oportuna e subordinada ao interesse público;
>
> VI - utilização de informações relevantes e de qualidade para apoiar o funcionamento dos processos de riscos e dos controles internos da gestão;
>
> VII - disseminação de informações necessárias ao fortalecimento da cultura e da valorização da gestão de riscos e dos controles internos da gestão;
>
> VIII - realização de avaliações periódicas para verificar a eficácia da gestão de riscos e dos controles internos da gestão, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive a alta administração;
>
> IX - gestão de riscos e controles internos da gestão suportada por níveis adequados de exposição a riscos;

X - integração e utilização das informações e resultados gerados pela gestão de riscos e controles internos da gestão na elaboração do planejamento estratégico, na tomada de decisões e na melhoria contínua dos processos organizacionais;

XI - aderência dos métodos e modelos de gerenciamento de riscos às exigências regulatórias;

XII - gestão dinâmica, interativa, capaz de reagir às mudanças e alinhada ao contexto e ao perfil de risco da instituição; e

XIII - gestão transparente e inclusiva, com a incorporação dos fatores humanos e culturais.

[…]

Nesse sentido, o objetivo da presente Metodologia é estabelecer o fluxo das ações internas que auxilie na identificação e mitiguem as ameaças e vulnerabilidades desta Autarquia, permitindo uma melhor tomada de decisão.

4. COMPETÊNCIAS SOBRE A GESTÃO DE RISCOS

4.1. O Modelo de Três Linhas proposto pelo The Institute of Internal Auditors (IIA) ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos. Em relação às competências, a Sudeco adotará a estrutura de três linhas e IN CGU/MP nº 01/2016 da seguinte forma:

1ª Linha: Controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, nos macroprocessos finalísticos e de apoio. Na Sudeco, a 1ª linha de defesa da Gestão da Governança, Riscos e Controles Internos é composta pelo superintendente, diretores, chefe de gabinete, coordenadores-gerais, ouvidor, corregedor, coordenadores, chefes de divisão, chefes de serviço e responsáveis pelos processos de trabalho, projetos e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais.

2ª Linha: Supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e compliance. Neste nível atuam o Comitê de Governança, Riscos, Controles e Integridade - CGRCI, o Núcleo de Gestão de Riscos e Controle - NGRC e a Unidade de Gestão da Integridade-UGI. O CGRCI é o órgão colegiado de decisão máxima na estrutura de governança da Sudeco, constituído pelo Superintendente, que o preside, e do titular da Diretoria de Administração (DA), Diretoria de Implementação de Programas e Gestão de Fundos (DIPGF), da Diretoria de Planejamento e Avaliação (DPA) e Ouvidoria. O NGRC é responsável pelo apoio técnico, de forma permanente, ao Comitê e às unidades administravas da Sudeco durante todas as fases de gestão de riscos e controles.

3ª Linha: Constituída pela Auditoria interna no âmbito da Sudeco, uma vez que esta é responsável por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa) e da supervisão dos controles internos (segunda linha ou camada de defesa). Compete à Auditoria-Geral da Sudeco fornecer à alta administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização e prover avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos.

Figura 1: Modelo das Três Linhas
Fonte: Modelo das Três Linhas do IIA 2020

4.1.1. **Competências do Comitê de Governança, Riscos, Controles e Integridade da Superintendência do Desenvolvimento do Centro-Oeste – CGRCI** (art. 2°, Portaria n° 150, de 17 de maio de 2018)

- Promover práticas e princípios de conduta e padrões de comportamentos;
- Institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;
- Promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, integridade, gestão de riscos e controles internos;
- Garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
- Promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;
- Promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações, na forma da lei;
- Adotar e aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
- Supervisionar o mapeamento e a avaliação dos riscos chave (riscos críticos) que podem comprometer a prestação de serviços de interesse público;

- Liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no âmbito da Sudeco;
- Estabelecer limites de exposição a riscos globais da Instituição, bem como os limites de alçada ao nível de unidade, política pública, ou atividade;
- Aprovar e supervisionar método de priorização de temas e macroprocessos na estrutura organizacional para gerenciamento de riscos e implementação dos controles internos da gestão;
- Emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos administrativos, e
- Monitorar e aprimorar suas próprias recomendações e deliberações.

4.1.2. **Competências do Núcleo de Gestão de Riscos e Controle – NGRC**

- Propor a Metodologia de Gestão de Riscos e suas revisões;
- Definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- Realizar e acompanhar estudos de novas metodologias e tecnologias quanto a possíveis impactos na Gestão de Riscos;
- Propor normas relativas à Gestão de Riscos e Controles Internos e suas revisões;
- Oferecer capacitação continuada em Gestão de Riscos para os servidores da Sudeco;
- Auxiliar a alta administração na implementação e na manutenção de processos, estruturas e mecanismos adequados a incorporação dos princípios e das diretrizes da governança;
- Propor recursos necessários às ações do Comitê;
- Coordenar as atividades deliberadas pelo Comitê, acompanhar e orientar no tratamento dos riscos mapeados pelos gestores responsáveis da unidades administrativas;
- Propor reuniões ordinárias e extraordinárias ao Comitê;
- Apoiar tecnicamente as reuniões e demais atividades do Comitê, incluindo o acompanhamento da execução de suas deliberações;
- Solicitar assessoria técnica e informações às unidades da Sudeco para subsidiar análises e decisões do CGRCI;
- Prestar orientação técnica às unidades administravas da Sudeco sobre o tema da Gestão de Riscos e Controles Internos;
- Atuar como facilitador na integração dos responsáveis pela Gestão de Riscos;
- Consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Governança, Riscos, Controles e Integridade, e
- Coordenar e acompanhar todas as fases do processo de gestão de riscos.

4.1.3. **Competências dos Gestores de Riscos** (art. 8°, Resolução n° 15, de 16 de outubro de 2017)

- Assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da Sudeco;
- Monitorar o risco de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos instituída; e
- Garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da instituição.

4.2. **Integração dos Processos Organizacionais**

Um dos princípios da Política de Gestão de Riscos da Sudeco é a integração e utilização das informações e resultados gerados pela gestão de riscos e controles internos da gestão na elaboração do plano estratégico, na tomada de decisões e na melhoria contínua dos processos organizacionais.

Portanto, cada Diretoria desta Superintendência deverá elaborar seu Plano de Gestão de Riscos, com a identificação dos processos organizacionais sob sua responsabilidade contendo todas as etapas da Gestão de Riscos, detalhadas nesta Metodologia. Estes Planos serão compilados e apresentados ao CGRCI desta Superintendência, pelo Núcleo de Gestão de Riscos e Controle, ao final de cada ciclo de gestão definidos no Plano de Gestão de Riscos e Controles Internos.

Para definir os critérios de seleção dos riscos a serem tratados, o Plano de Gestão de Riscos, informa que devem ser priorizados os Macroprocessos informados no Plano Estratégico da Sudeco e o art. 5°, inciso VII da Política de Gestão de Riscos, destaca que um dos objetivos desta Autarquia é aumentar a probabilidade de alcance dos objetivos institucionais, reduzindo os riscos a níveis aceitáveis.

5. PROCESSO DE GESTÃO DE RISCOS

Segundo o item 5 da ABNT ISO 31000:2009, o processo de gestão de riscos deve ser parte integrante da gestão, incorporado na cultura e nas práticas, e adaptado aos processos de negócios da organização, conforme demonstrado na figura 2.

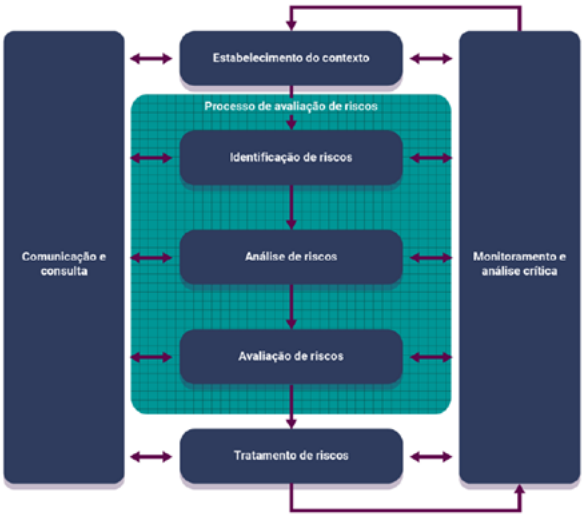


Figura 2: Processo de gestão de riscos segundo a ISO 31000.
Fonte: Material Gestão de Riscos no Setor Público - ENAP

Os métodos e critérios para priorizar os processos de trabalho serão indicados pelos Gestores de Riscos.

Uma vez priorizados os processos de trabalho, dar-se-á início ao processo de Gestão de Riscos, composto por atividades que interagem de forma cíclica: levantamento do ambiente e dos objetivos, identificação de eventos de riscos, avaliação de eventos de riscos e controles, resposta ao risco e informação e comunicação e monitoramento.

Essas atividades serão realizadas no Sistema Agatha, solução tecnológica específica, criada para auxiliar o processo de gerenciamento de riscos.

5.1. Solução Tecnológica

O Sistema Agatha (Sistema de Gestão de Integridade, Riscos e Controles), consiste em uma ferramenta automatizada, desenvolvida para auxiliar o processo de gerenciamento de riscos e controle, desenvolvido pelo então Ministério do Planejamento, Desenvolvimento e Gestão, substituído pelo Ministério da Economia e disponibilizado gratuitamente aos órgãos interessados da Administração Pública.

Será adotado pela Sudeco, e seus desdobramentos de fases da gestão de riscos e controles internos serão realizadas por meio dele, o qual será complementado com Relatório Semestral.

O Relatório Semestral auxiliará as unidades no acompanhamento do desempenho do Plano de Gestão de Riscos como um todo e deverá ser encaminhado às partes interessadas, NGRC e CGRCI, contendo as seguintes seções:

a) Introdução;
b) Estrutura Organizacional da unidade;
c) Processos avaliados na unidade;
d) Metodologia aplicada;
e) Documentos de referência;
f) Período de avaliação;
g) Riscos identificados;
h) Ações de controle propostas;
i) Avaliação dos Controles;
j) Considerações Finais*; e
k) Anexos, se necessários.

*O relatório deverá conter nas Considerações Finais, parecer sobre os riscos e controles identificados nos processos, principalmente, no que se refere a riscos relevantes.

5.2. Metodologia de Gestão de Riscos

A Metodologia de Gestão de Riscos a ser utilizada na Sudeco é composta por cinco etapas, conforme ilustrado de forma resumida na figura 3 abaixo:

Figura 3: Etapas da Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão.
Fonte: Material Gestão de Riscos no Setor Público - ENAP

Ela tem por finalidade orientar a identificação, avaliação e a resposta aos riscos dos processos das unidades, bem como instruir sobre o seu monitoramento e avaliação.

O gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas e processos de trabalho, sendo priorizados os processos organizacionais que impactam diretamente na consecução dos objetivos estratégicos definidos no Plano Estratégico da Sudeco, conforme exemplificado no anexo IV que apresenta o fluxo do processo de gerenciamento de riscos da Sudeco.

5.2.1. **Etapa 1 – Levantamento do Ambiente e dos Objetivos (Estabelecimento do Contexto)**

A análise do ambiente tem a finalidade de colher informações para apoiar a identificação de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas com o intuito de assegurar o alcance dos objetivos do macroprocesso/processo.

Aqui são identificados os objetivos estratégicos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos.

A fixação de objetivos, refere-se à entrega adequada de produtos e serviços à sociedade, plenamente alinhados à missão, visão, valores, e ao propósito.

Dessa forma, o dirigente máximo da Diretoria deve identificar e priorizar os processos organizacionais, observando o critério estabelecido no art 5° da Política de Gestão de Riscos da Sudeco.

Como fonte de auxílio a esta primeira etapa de identificação de forças e fraquezas (pontos fortes e pontos fracos), bem como para a análise e registro das possíveis influências do ambiente externo sobre o macroprocesso/processo quanto a oportunidades e ameaças (pontos fortes e pontos fracos), sugere-se a utilização da ferramenta Análise de SWOT.

A imagem abaixo sintetiza a aplicação da análise SWOT:

Figura 4: Análise de SWOT
Fonte: Material Gestão de Riscos no Setor Público - ENAP

Análise SWOT é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente). As informações obtidas sobre o ambiente interno e externo contribuem para a identificação dos riscos e para a escolha das respostas aos riscos.

5.2.1.1. **Contexto do Processo Organizacional**

Dessa forma, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo, devendo ser identificados pelo menos:

- Descrição resumida do processo: breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional: destacar quais objetivos são alcançados pelo processo organizacional. Sendo possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas como estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão “O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?”;

- Relação dos Objetivos Estratégicos da Sudeco relacionados ao processo;
- Periodicidade máxima do ciclo do processo de gerenciamento de riscos (conforme art. 10º, da Política de Gestão de Riscos da Sudeco). A unidade deve propor qual o prazo necessário para a um novo gerenciamento de riscos do processo organizacional;
- Unidade demandante do processo de gerenciamento de riscos no processo organizacional (a própria unidade ou o CGRCI, por exemplo);
- Justificativa para o processo de gerenciamento de riscos no processo. Apresentar os motivos que levaram a implementar a gestão de riscos no processo organizacional.
- Unidade responsável pelo processo organizacional;
- Leis e regulamentos relacionados ao processo organizacional;
- Sistemas tecnológicos que apoiam o processo organizacional;
- Partes interessadas no processo, podendo ser internas ou externas;
- Informações sobre o contexto externo do processo, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes; e
- Apetite a risco da unidade para o processo organizacional, caso seja diferente do definido neste documento.

No estabelecimento do contexto externo, importa especialmente descrever as relações da organização com as partes interessadas externas e as percepções destas acerca do valor criado. No estabelecimento do contexto interno, deve-se descrever os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização ou daquelas partes em que o processo de gestão de riscos pode ser aplicado (ABNT, 2009).

5.2.2. Etapa 2 - Identificação de eventos de riscos (Identificação dos Riscos)

Esta etapa tem por finalidade identificar e registar tanto os eventos de riscos que comprometem o alcance do objetivo do processo, como as causas e os efeitos/consequências de cada um deles.

Por meio da identificação de eventos de riscos (figura 4), pode-se planejar a forma de tratamento adequada e qual o tipo de resposta a ser dada a esse risco.

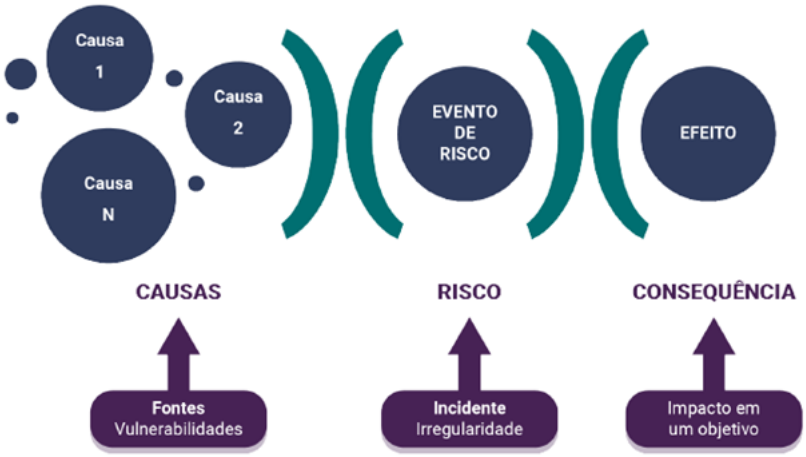


Figura 5: Componentes do Evento de Risco.
Fonte: Material Gestão de Riscos no Setor Público - ENAP

Além disso, é necessário identificar nessa etapa, o responsável pelo gerenciamento de cada evento de risco e a equipe técnica que participará do processo de gerenciamento do(s) risco(s).

Tendo em vista que para a identificação dos eventos de riscos se faz necessária a verificação das causas e consequências para registro no Sistema Agatha, a presente Metodologia sugere a utilização do Método bow-tie:

Método Bow-tie: Trata-se de uma forma **esquemática** e simples de descrever e analisar os caminhos de um risco, desde as suas causas até as suas consequências. O foco dessa técnica está nas barreiras entre as causas e o risco e, o risco e suas consequências.

O método consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que um problema pode estar relacionado a diversas causas e consequências.

A figura abaixo demonstra essa técnica para melhor compreensão.

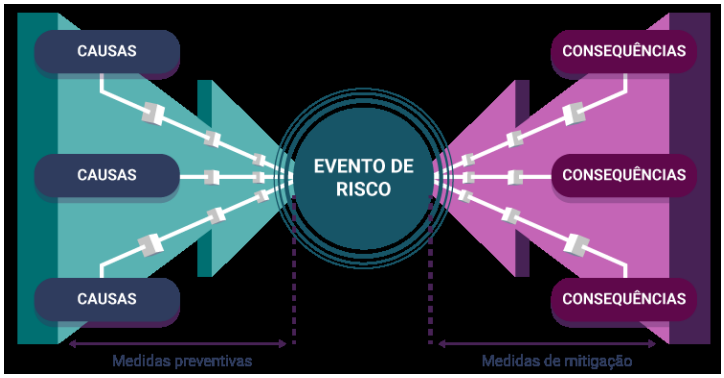


Figura 6: Método Bow-Tie
Fonte: Material Gestão de Riscos no Setor Público - ENAP

A sintaxe a seguir, auxilia no desenvolvimento desta etapa para a descrição de um evento risco:

Devido a <CAUSA/FONTE>, poderá acontecer <DESCRIÇÃO DO EVENTO DE RISCO>, o que poderá levar a <DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS> impactando no <OBJETIVO DE PROCESSO >.

Como forma complementar ao método Bow-tie, outras técnicas podem ser utilizadas na identificação de eventos de riscos. Dentre as outras técnicas, podemos citar os questionários, checklist, whorkshop, inspeções e auditorias, fluxogramas e:

- **Brainstorming**: Técnica de geração de ideias em grupo, na qual os participantes apresentam o maior número possível de opiniões. Essa técnica é composta de quatro regras básicas: a) as críticas devem ser descartadas – a avaliação das percepções deve ser guardada para momentos posteriores; b) a geração livre do entendimento deve ser encorajada; c) foco na quantidade – quanto maior o número de ideias, maiores as chances de se ter ideias válidas; d) combinação e aperfeiçoamento de ideias geradas pelo grupo.
- **Delphi**: Consiste basicamente na aplicação de um questionário preparado por um facilitador, a um grupo de especialistas, cujas respostas são acumuladas em um único documento. Em seguida o documento é apresentado ao grupo de especialistas para uma nova rodada de considerações, caracterizando a interação do método, que busca a convergência de opiniões sem que os especialistas se conheçam entre si.
- **Análise SWOT:** Ferramenta de planejamento estratégico, utilizada para análise de projetos e/ou negócios, ou em qualquer outra situação que envolva uma decisão. A aplicação dessa técnica consiste na avaliação do projeto sob cada uma das quatro perspectivas: forças, fraquezas, oportunidades e ameaças, relavas aos ambientes interno e externo, geralmente apresentadas em forma de quadrantes.
- **Diagrama de causa e efeito**: Também conhecido como diagrama espinha de peixe é uma ferramenta utilizada para a análise de dispersões no processo. O objetivo é representar a relação entre um "efeito" e suas possíveis "causas". Esta técnica é utilizada para descobrir, organizar e resumir conhecimento de um grupo a respeito das possíveis causas que contribuem para um determinado efeito.

5.2.2.1. **Tipologias dos Riscos/Categoria dos Riscos**

Com o resultado da etapa do Contexto do Processo Organizacional, deve-se construir uma lista de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

Os eventos de riscos podem ser identificados a partir de perguntas, como:

- O evento é um risco que pode comprometer (evitar, atrasar, prejudicar ou impedir) claramente um objetivo do processo?
- O evento é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
- O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?

Para eventos **identificados e analisados como riscos do processo**, deve-se indicar:

- Objetivo do processo organizacional/etapa impactado pelo risco;
- Causas: motivos que podem promover a ocorrência do risco;
- Efeitos/Consequências: resultados do risco que afetam os objetivos; e
- Categorias dos riscos (art. 6°, § 1°da Resolução n° 15, de 16 de outubro de 2017), dividido em:

I - **Riscos Estratégicos:** eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da unidade/órgão, caso venham ocorrer;

II - **Riscos Operacionais:** eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

III - **Riscos Financeiros/Orçamentários:** eventos que podem comprometer a capacidade do órgão ou entidade de contar com os 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 e de convênios;

IV - **Riscos de Imagem/Reputação do Órgão:** eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;

V - **Riscos de Integridade:** eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos;

VI - **Riscos Fiscais:** eventos que podem afetar negativamente o equilíbrio das contas públicas; e

VII - **Riscos Legais/Conformidade:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.

O anexo II deste documento apresenta o modelo de planilha para o registro de informações produzidas nas etapas de Estabelecimento de Contexto e Identificação dos Riscos para ser utilizado como forma auxiliar ao sistema Agatha, caso seja necessário.

5.2.3. **Etapa 3 - Avaliação de Eventos de Riscos e Controles (Análise dos Riscos)**

Esta etapa tem por finalidade avaliar os eventos de riscos identificados, considerando as suas causas e consequências. Os eventos devem ser avaliados sob a perspectiva de Probabilidade x Impacto. Normalmente as causas estão relacionadas à probabilidade de o evento ocorrer e as consequências ao impacto, caso o evento se materialize.

A avaliação de riscos deve ser realizada por meio de análises quantitativas e qualitativas ou uma combinação de ambas e, ainda, quanto à sua condição de inerentes (sem considerar qualquer controle) e residuais (considerando os controles identificados e avaliados quanto ao desenho e a sua execução).

Os conceitos de risco inerente, residual e controles internos da gestão estão explícitos na IN Conjunta MP/CGU Nº 01/2016), quais sejam:

> […]
>
> Risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016).
>
> Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco (Art. 2º, XV, IN Conjunta MP/CGU Nº 01/2016).
>
> Controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade (Art. 2º, V, IN Conjunta MP/ CGU Nº 01/2016).
>
> […]

Os quadros 01 e 02 trazem as escalas de probabilidade e impacto, respectivamente:

Probabilidade	Descrição da probabilidade, desconsiderando os controles	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	5

Quadro 01: Escala de Probabilidade
Fonte: Elaborado pela Astecgab

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	3
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	4
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	5

Quadro 02: Escala de Impacto
Fonte: Elaborado pela Astecgab

Para determinação do impacto (figura 7), é necessário ainda, analisar e atribuir pesos aos fatores que estão intrínsecos e ligados em cada evento de riscos:

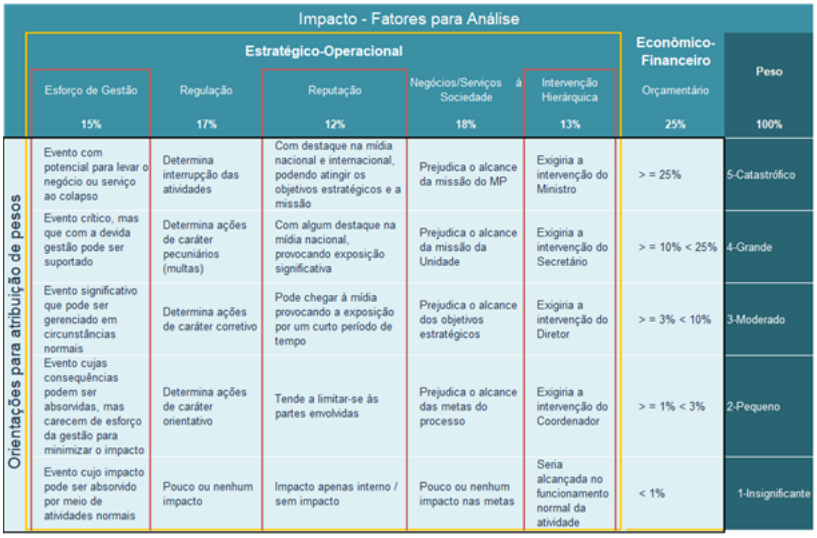


Figura 7: Impacto – Fatores para análise
Fonte: Material Gestão de Riscos no Setor Público - ENAP

A multiplicação entre os valores de probabilidade e impacto define o nível do risco inerente, ou seja, o nível antes de considerar as respostas que a Administração adota para reduzir a probabilidade do evento ou os seus impactos nos objetivos.

RI = NP x NI Em que: **RI** = nível do risco inerente **NP** = nível de probabilidade do risco **NI** = nível de impacto do risco

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas:

Figura 8: Matriz de Riscos
Fonte: Material Gestão de Riscos no Setor Público - ENAP

Após a classificação do evento na Matriz de Risco, a equipe deve descrever os controles existentes, que atuam sobre as possíveis causas do risco com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos/checklist definidos para o processo e capacitação dos servidores envolvidos no processo;

Em seguida, a equipe técnica designada deve avaliar a eficácia dos controles existentes em relação aos objetivos do processo organizacional. Ou seja, se os controles apontados durante a etapa de Identificação e Análise do risco têm auxiliado no tratamento adequado deste. O quadro 03 mostra os níveis de avaliação dos controles existentes:

Nível	Descrição	Fator de Avaliação dos Controles
Inexistente NC=0%	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco NC=20%	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano NC=40%	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório NC=60%	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte NC=80%	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

Quadro 03: Níveis de Avaliação dos Controles Internos Existentes
Fonte: Elaborado pela Astecgab

Após o risco inerente ser mensurado, é necessário identificar e avaliar os controles quanto ao seu desenho e à sua operação, que respondam aos eventos de riscos identificados.

Quanto ao desenho, são verificadas as seguintes informações:

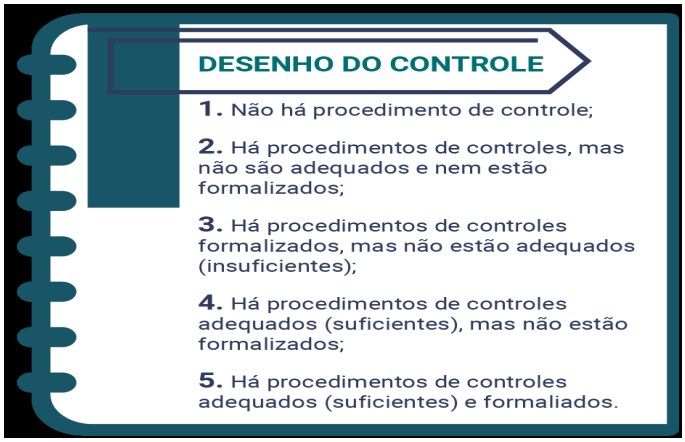


Figura 9: Desenho do Controle

Quanto à operação, as informações a serem analisadas são:

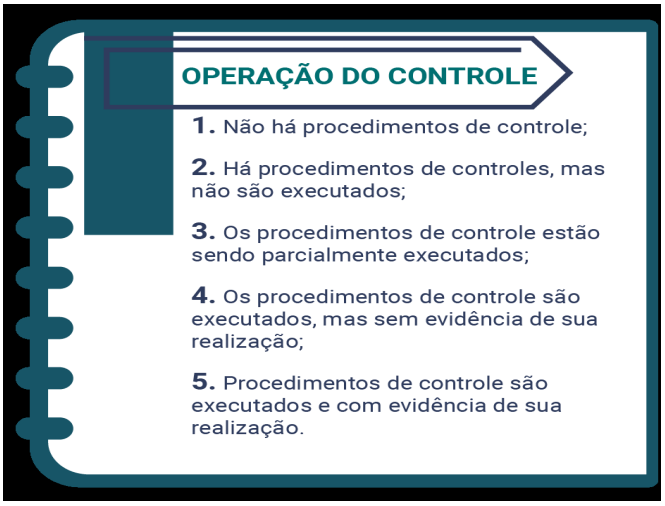


Figura 10: Operação do Controle

O valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles, corresponde ao nível de risco residual, conforme abaixo:

RR = RI x FC
Em que:
RR = nível do risco residual
RI = nível do risco inerente
FC = fator de avaliação dos controles existentes

O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida para o risco inerente, e o Anexo II deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Análise dos Riscos.

5.2.4. **Etapa 4 – Resposta ao Risco (Tratamento dos Riscos)**

Nesta etapa são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas.

5.2.4.1. **Priorização dos Riscos**

Para priorizar os riscos devemos considerar os valores dos níveis de riscos residuais calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento.

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. O quadro 04 mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Classificação	Ação necessária	Exceção
Risco Pequeno	Nível de risco **dentro do apetite a risco**, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de t essa priorização deve ser justificada pela unidade e aprovada pelo máximo da Diretoria.
Risco Moderado	Nível de risco **dentro do apetite a risco.** Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de t essa priorização deve ser justificada pela unidade e aprovada pelo máximo da Diretoria.
Risco Alto	Nível de risco **dentro do apetite a risco**. Qualquer risco nesse nível deve ser comunicado ao CGRCI e ao dirigente máximo da Diretoria e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da Diretoria.	Caso o risco não seja priorizado para implementação de medidas tratamento, a não priorização deve ser justificada pela unidade e pelo dirigente máximo da Diretoria.
Risco Crítico	Nível de risco muito **além do apetite a risco.** Qualquer risco nesse nível deve ser comunicado ao CGRCI e à Alta Administração para uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.	Caso o risco não seja priorizado para implementação de medidas tratamento, a não priorização deve ser justificada pela unidade e pelo seu dirigente máximo e pelo CGRCI.

Quadro 04: Atitude perante o risco para cada classificação
Fonte: Elaborado pela Astecgab

Segundo o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do antigo Ministério do Planejamento, Desenvolvimento e Gestão - MP, o Apetite a Risco é a quantidade de risco, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor, ou seja, refere-se ao máximo nível de risco que uma organização está disposta a correr para atingir seus objetivos estratégicos.

O Plano de Gestão de Riscos e Controles Internos, determinará o Apetite a Risco da Sudeco para cada Ciclo de Gestão de Riscos como também sua periodicidade.

O Anexo II deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Priorização de Riscos a ser utilizado de forma auxiliar ao Sistema Agatha, caso seja necessário.

5.2.4.2. **Definição de Resposta aos Riscos**

O objetivo desta etapa é definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa anterior.

Para todos os riscos identificados, é necessário definir as possíveis respostas (evitar, compartilhar/transferir, reduzir ou aceitar), conforme as opções de tratamento descritas abaixo:

- **Evitar:** É a decisão de não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco.
- **Reduzir:** Consiste em adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos. Essas ações/procedimentos são denominadas de controle interno.
- **Compartilhar/Transferir:** É mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio. Um risco transferido não é eliminado, este ainda poderá se materializar e por isso deve ser monitorado.
- **Aceitar:** Decisão de não realizar nenhuma ação mitigadora para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização.

É importante que, em uma primeira abordagem da elaboração das respostas aos riscos, avalie-se a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, que devem ser pactuados com o intuito de diminuir o impacto de suas consequências, podendo estes serem preventivos ou corretivos.

As ações para responder aos eventos de riscos devem ser compatíveis com a tolerância a riscos definidas no início de cada processo, considerar a relação custo benefício, refletir se o efeito da resposta afeta a probabilidade ou o impacto, ou ambos, e designar um responsável pelas respostas (proprietário do risco).

Se as iniciativas de resposta aos riscos envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano de Gestão de Riscos para que essas unidades validem as iniciativas de que participarem.

O Anexo III deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Resposta aos Riscos.

5.2.4.3. **Plano de Tratamento**

O Plano de Tratamento é um conjunto de ações necessárias para adequar os níveis de riscos, por meio da adoção de novos controles ou da otimização dos controles atuais do processo, estabelecendo atividades para assegurar que a resposta seja conduzida.

O referido Plano deve apresentar as medidas de tratamento dos riscos do processo organizacional, contendo:

- **Controle Proposto:** controles ou ações para responder ao evento de risco;
- **Tipo de controle proposto:** preventivo (atua na causa) ou corretivo (atenua o efeito);
- **Objetivo do controle:** melhoria de controle existente ou adotar controle novo;
- **Área responsável pela implementação do controle:** gestor do processo ou servidor designado;
- **Como será implementado:** informar se por meio de projeto, melhoria em sistema, criação de norma, plano de contingência, etc.;
- **Intervenientes:** outras áreas ou servidores intervenientes na ação;
- **Data de início:** informa data prevista do início; e
- **Data da conclusão:** informar data prevista para a conclusão.

As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, podem vir a prevenir ou administrar os riscos inerentes ou em potencial da entidade. São exemplos de atividades de controle que podem ser utilizados no Plano de Tratamento:

- 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, e
- Revisão de desempenho operacional.

No sistema Agatha é realizado o acompanhamento do Plano de Tratamento durante sua execução, podendo ser incluído para cada ação um novo acompanhamento, informando-se o status do plano de ação (a iniciar, iniciado, concluído ou cancelado), se o controle foi implementado como planejado (sim, não ou parcialmente), e as justificativas/ações realizadas ou observações.

Os controles devem ser propostos, ainda, sob a ótica de custo/benefício com o objetivo de otimizá-los. O custo de um controle não deve ser mais caro do que o benefício gerado por ele.

5.2.4.4. **Validação dos Resultados das Etapas 1 a 4 da Metodologia da Gestão de Riscos e Controles Internos**

Os resultados das etapas anteriores da Metodologia (Levantamento do Ambiente e dos Objetivos, Identificação de eventos de riscos, Avaliação de Eventos de Riscos e Controles e Resposta ao Risco) de cada Diretoria, deverão ser previamente analisados e aprovados pelo seu respectivo Diretor.

Após a aprovação desses resultados, o responsável pelo Plano ou o Dirigente da unidade deverá:

- Encaminhar os resultados ao Núcleo de Gestão de Riscos e Controle para análise, adequações e encaminhamento ao Comitê de Governança, Riscos, Controles e Integridade para avaliação e aprovação; e
- Encaminhar o Plano de Tratamento aprovado às Diretorias corresponsáveis pelas iniciativas para que essas também incluam as ações em seu Plano de Gestão de Riscos, caso haja ações realizadas de forma conjunta com outras diretorias.

5.2.4.5. **Implementação do Plano de tratamento**

A implementação do Plano de Tratamento envolve a participação da Diretoria responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

A responsabilidade primária pelo Plano de Tratamento permanece com a Diretoria responsável pelo processo organizacional e deve ser definido o principal responsável pela implementação da iniciativa (cargo), que também deverá monitorar e reportar a evolução ao NGRC e CGRCI quando solicitado.

5.2.5. **Etapa 5 – Informação, Comunicação e Monitoramento (quem é o responsável pelo controle)**

Segundo a ISO 31000:2009, durante todas as etapas do plano de gerenciamento de riscos, é importante a comunicação entre as partes interessadas, portanto, a Sudeco decidiu utilizar a Matriz de Responsabilidade RACI que define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos.

Segundo SOUZA e BRASIL (2017), são elementos da Matriz RACI:

- **Responsável:** quem executa a atividade;
- **Autoridade:** quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;
- **Consultado:** quem pode agregar valor ou é essencial para a implementação; e
- **Informado:** quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Durante as etapas do processo de gerenciamento de riscos, é importante que a comunicação observe os agentes ou unidades apontadas como consultados ou informados na Matriz RACI do quadro 05.

	Comitê de Governança, Riscos, Controles e Integridade - CGRCI	Núcleo de Gestão de Riscos e Controle	Dirigente Máximo da Unidade (ex.: Diretor)	Responsável pelo Gerenciamento de Riscos*	Equipe Técnica Designada**	Responsável pela Implementação***	Cargo****
Definir Plano de Gestão de Riscos da Diretoria	A	C	R	C	I	I	I
Selecionar um Processo Organizacional	A	I	R	C	I	I	-
Realizar o Estabelecimento do Contexto (Etapa 1)	I	C	A	R	R	-	-
Realizar a Identificação dos Riscos (Etapa 2)	I	C	A	R	R	-	-
Realizar a Análise dos Riscos (Etapa 3)	I	C	A	R	R	-	-
Realizar a Priorização dos Riscos (Etapa 4)	I	C	A	R	R	-	-
Realizar a Definição de Respostas aos Riscos (Etapa 4)	I	C	A	R	R	-	-
Validar os Riscos Levantados (Etapa 4)	I	C	R	C	C	-	-
Implementar o Plano de Tratamento (Etapa 4)	I	C	A	I	C	R	-
Monitorar (Etapa 5)	I/R	C	A	R	I	C	R
Realizar Avaliação Estratégica	A	R	C	C	R	-	-

Quadro 05: Matriz RACI para o processo de gestão de riscos da Sudeco
Fonte: Elaborado pela Astecgab

* Para cada Processos Organizacional, deverá ser designado pelo Dirigente Máximo da Unidade um Responsável pelo Gerenciamento de Riscos (cargo);
** Todas as Diretorias deverão ter sua própria Equipe Técnica Designada pelo Dirigente Máximo da Unidade para tratar da Gestão de Riscos desta Diretoria;
*** Responsável pela implementação será definido pelo Dirigente Máximo da Unidade;
**** Responsável por monitorar o Plano de Gestão de Riscos da Diretoria.

O Dirigente máximo da unidade fica responsável por definir o Responsável pelo Gerenciamento de Riscos da Unidade, bem como a Equipe Técnica, o Responsável pela Implementação e o servidor responsável por monitorar o Plano de Gestão de Riscos de cada Diretoria. As eventuais mudanças identificadas durante o monitoramento devem ser encaminhadas ao Núcleo de Gestão de Riscos e Controle, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos.

5.2.5.1. **Monitoramento e Análise Crítica**

As atividades de monitoramento e análise crítica serão realizadas pela unidade responsável pelo processo de forma contínua, para assegurar que o registro de riscos seja mantido atualizado, bem como que nele sejam documentados os resultados das ações.

Para permitir o melhor acompanhamento do gerenciamento de riscos, as unidades deverão estabelecer indicadores que permitam aferir sua implementação e os resultados dos controles apresentados para a redução dos riscos, elencando no mínimo o objetivo do controle, o indicador e a forma de apuração de resultado.

Desta forma, a título exemplificativo e não exaustivo, os indicadores descritos na lista abaixo, podem ser utilizados no acompanhamento e reporte dos riscos.

Indicador	Fórmula
% processos mapeados por unidade	processos mapeados/total de processos
% processos essenciais mapeados por unidade	processos essenciais mapeados/processos essenciais
% processos relevantes mapeados por unidade	processos relevantes mapeados/processos essenciais
% processos moderados mapeados por unidade	processos moderados mapeados/processos essenciais
% processos essenciais com riscos mapeados por unidade	processos essenciais com riscos mapeados/processos essenciais
% processos relevantes com riscos mapeados por unidade	processos relevantes com riscos mapeados/processos relevantes
% processos moderados com riscos mapeados por unidade	processos moderados com riscos mapeados/processos moderados
% controles implementados por processo	controles concluídos/total de controles do processo
% controles em andamento por processo	controles em andamento/total de controles do processo
% controles atrasados por processo	controles atrasados/total de controles

Quadro 06: Indicadores de Monitoramento
Fonte: Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.
Ministério do Planejamento, Desenvolvimento e Gestão e Assessoria Especial de Controle Interno

Com base nesse monitoramento serão elaborados Relatórios Semestrais, os quais serão encaminhados pelas unidades ao NGRC contendo minimamente as seções elencadas no item 7.1 desta Metodologia.

Semestralmente, o Núcleo de Gestão de Riscos e Controle produzirá relatório com o resultado do acompanhamento das ações relacionadas ao Plano de Gestão de Riscos de cada unidade, que será enviado para avaliação do Comitê de Governança, Riscos, Controles e Integridade – CGRCI. Portanto, cada unidade deverá encaminhar seu relatório ao NGRC até o último dia útil dos meses de junho e dezembro para a compilação das informações pelo Núcleo e aprovação do Relatório pelo CGRCI, que deverá ocorrer em até 30 dias, e, caso necessário, esse prazo poderá ser prorrogado por mais 30 dias desde que justificado.

Caso sejam identificadas deficiências ou vulnerabilidades, serão feitas recomendações por estas instâncias para aperfeiçoamento dos instrumentos de gestão riscos e controles.

Mudanças identificadas durante o monitoramento devem ser encaminhadas ao Diretor de cada unidade organizacional, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos da sua Diretoria.

5.2.5.2. **Comunicação e Consulta**

O acesso a informações confiáveis, íntegras e tempestivas é vital para o gerenciamento de riscos e controles internos. Todos os atos relativos à governança, riscos e controles internos serão registrados no Sistema Eletrônico de Informações – SEI, além de estarem no Sistema de Gestão de Riscos – Agatha e de acordo com os processos priorizados para tal.

A Metodologia de Gestão de Riscos e Controles Internos da Sudeco terá validade até 31 de dezembro de 2021 e suas atualizações ocorrerão a partir do exercício de 2022, de acordo com o ciclo do Planejamento Estratégico. No entanto, poderá ser revisto a qualquer tempo, sempre que identificado um novo risco, por proposição de qualquer dos membros do Comitê conforme § 2º do art. 10° da Resolução n° 15 de 16 de outubro de 2017 que dispõe sobre a instituição da Política de Gestão de Riscos da Superintendência do Desenvolvimento do Centro-Oeste – Sudeco.

O Núcleo de Gestão de Riscos e Controle comunicará periodicamente os resultados do acompanhamento das ações relacionadas a Metodologia da Gestão de Riscos e Controles Internos, que será apresentado ao Comitê de Governança, Riscos, Controles e Integridade e à Sudeco como um todo.

5.2.5.3. **Controle e Avaliação**

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

O controle e a avaliação do gerenciamento de riscos e seus resultados serão realizados por meio do Sistema Agatha, o qual dispõe de módulos correspondentes a todas as fases.

O NGRC acompanhará o detalhamento das informações por meio de relatórios, de acordo com o anteriormente disposto nesta Metodologia e orientará as unidades quando necessário.

6. CONSIDERAÇÕES FINAIS

A Gestão de Riscos, Controles Internos e Integridade, quando devidamente implementados, é um elemento essencial para a boa governança.

Importante ressaltar que, mesmo um processo bem estruturado de gerenciamento de riscos não está totalmente imune a incertezas, mas certamente o impacto e a probabilidade de eventuais ameaças serão substancialmente reduzidos e mais oportunidades poderão ser aproveitadas.

A presente Metodologia de Gestão de Riscos e Controles Internos da Superintendência do Desenvolvimento do Centro-Oeste – Sudeco visa amparar a gestão de risco desta Autarquia, contribuindo com a implantação de boas práticas de gestão para a tomada de decisões e apoiar de forma decisiva as ações que permitirão à Sudeco cumprir sua missão, visão, propósito e valores consignados no Planejamento Estratégico.

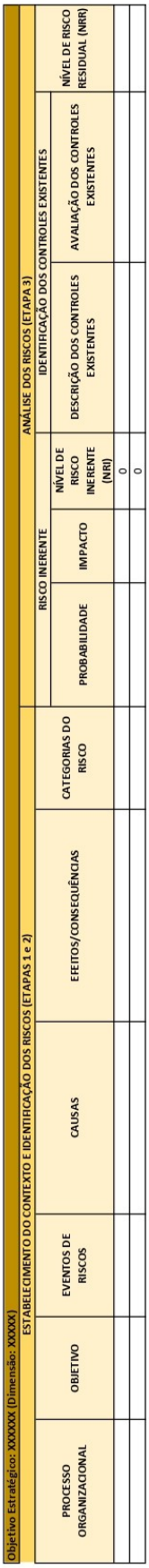
7. INSTRUMENTOS DA ESTRUTURA DE GESTÃO DE RISCOS E CONTROLES

Os instrumentos que fazem parte da Gestão de Riscos e Controles na Sudeco são:

- Resolução n° 12, de 13 de setembro de 2017 que aprova o Regimento Interno do Comitê de Governança, Riscos e Controles da Superintendência do Desenvolvimento do Centro-Oeste – Sudeco.
- Resolução n° 15, de 16 de outubro de 2017 que dispõe sobre a Política de Gestão de Riscos;
- Portaria n° 150, de 17 de maio de 2018 que Institui o Comitê de Governança, Riscos, Controles e Integridade e o Programa de Integridade no âmbito da Superintendência do Desenvolvimento do Centro-Oeste – Sudeco;
- Plano de Gestão de Riscos e Controles Internos;
- Metodologia da Gestão de Riscos e Controles Internos;
- Solução Tecnológica Sistema Agatha, e
- Manuais, cujos objetivos prioritários são fornecer diretrizes, princípios, orientações e operacionalização de processos.

ANEXO II

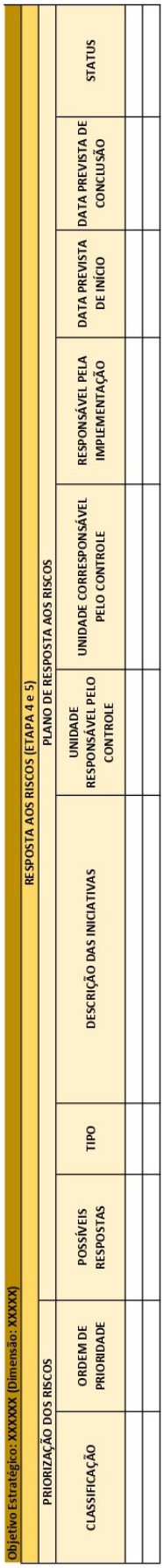
Modelo de Planilha de Apoio a Metodologia da Gestão de Riscos e Controles Internos



Objetivo Estratégico: XXXXXX (Dimensão: XXXXX)														
ESTABELECIMENTO DO CONTEXTO E IDENTIFICAÇÃO DOS RISCOS (ETAPAS 1 e 2)							ANÁLISE DOS RISCOS (ETAPA 3)							
							RISCO INERENTE			IDENTIFICAÇÃO DOS CONTROLES EXISTENTES				
PROCESSO ORGANIZACIONAL	OBJETIVO	EVENTOS DE RISCOS	CAUSAS	EFEITOS/CONSEQUÊNCIAS	CATEGORIAS DO RISCO	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO INERENTE (NRI)	DESCRIÇÃO DOS CONTROLES EXISTENTES	AVALIAÇÃO DOS CONTROLES EXISTENTES	NÍVEL DE RISCO RESIDUAL (NRR)			
								0						
								0						

ANEXO III

Modelo de Plano de Resposta aos Riscos



Objetivo Estratégico: XXXXXX (Dimensão: XXXXX)												
RESPOSTA AOS RISCOS (ETAPA 4 e 5)												
PRIORIZAÇÃO DOS RISCOS		PLANO DE RESPOSTA AOS RISCOS										
CLASSIFICAÇÃO	ORDEM DE PRIORIDADE	POSSÍVEIS RESPOSTAS	TIPO	DESCRIÇÃO DAS INICIATIVAS	UNIDADE RESPONSÁVEL PELO CONTROLE	UNIDADE CORRESPONSÁVEL PELO CONTROLE	RESPONSÁVEL PELA IMPLEMENTAÇÃO	DATA PREVISTA DE INÍCIO	DATA PREVISTA DE CONCLUSÃO	STATUS		

ANEXO IV

Fluxo Contínuo do Gerenciamento de Riscos da Sudeco