MINISTÉRIO DO DESENVOLVIMENTO REGIONAL
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DA AMAZÔNIA
COMITÊ DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES - CGIRC

ATO Nº 03, DE 31 DE JANEIRO DE 2020

O PRESIDENTE DO COMITÊ DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES - CGIRC, considerando o previsto no art. 23 da Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016, e a Portaria nº 310/2019-SUDAM, de 17/09/2019;

Considerando ausência do quórum mínimo para realização de Reunião do CGIRC, por motivo de vacância dos cargos de Diretor de Planejamento e Articulação de Políticas e de Diretor de Administração;

Considerando, ainda, os fatos e fundamentos presentes no Processo nº CUP: 59004.000978/2019-01, especialmente o contido no Despacho Simples NGRC , doc. SEI nº 0194218, e no Despacho Simples SUPERIN, doc. SEI nº 0196817,

RESOLVE:

Art. 1º Aprovar *Ad Referendum* do Comitê de Governança, Integridade, Riscos e Contoles, a revisão do Plano de Governança, Riscos e Controles da Superintendência do Desenvolvimento da Amazônia-SUDAM, na forma do Anexo deste Ato.

Art. 2º Revogar a Resolução CGRC n° 03, de 19 de junho de 2018.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Paulo Roberto Correia da Silva
Presidente do CGIRC

Documento assinado eletronicamente por **Paulo Roberto Correia da Silva**, **Superintendente**, em 31/01/2020, às 17:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.sudam.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0227850** e o código CRC **296C16D1**.

ANEXO

PLANO DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES INTERNOS

1. APRESENTAÇÃO

A Superintendência do Desenvolvimento da Amazônia-Sudam tem por finalidade promover o desenvolvimento includente e sustentável em sua área de atuação, bem como a integração competitiva da base produtiva regional na economia nacional e internacional. É responsável pela execução de políticas públicas para redução de desigualdades regionais, com o propósito de minimizar os desníveis regionais, por meio de atração de investimentos, da implantação de projetos de investimentos e benefícios fiscais e de apoio às transferências voluntárias, mediante convênios e ajustes.

Para alcançar seus objetivos prioritários, faz-se necessário dispor de uma estrutura de governança e mecanismos de controle eficientes.

Porém, como todo ente privado ou governamental, a SUDAM está sujeita a se deparar com desafios, incertezas e riscos no curso dos seus processos de trabalho.

Risco pode ser entendido como evento com alguma probabilidade de ocorrência capaz de gerar impactos (positivos ou negativos) no alcance de um objetivo. Para enfrentar os riscos, a Sudam apresenta o atual Plano de Governança, Riscos e Controles Internos - PGIRC que tem como objetivo definir as estratégias para identificar, analisar, avaliar os

riscos, e adotar medidas eficazes para reduzir a probabilidade de ocorrência ou do seu impacto nos objetivos estratégicos e operacionais desta autarquia.

Espera-se que a implementação da gestão de riscos no âmbito da Sudam proporcione relevantes benefícios com o aumento da probabilidade de atingimento dos objetivos organizacionais; melhoria dos mecanismos de identificação de oportunidades e ameaças; melhoria da gestão de incidentes e de lacunas; aumento do nível de atendimento aos requisitos legais e normativos, enfim, resultará na melhoria da governança corporativa e, consequentemente, a entrega de bens e serviços de forma adequada e tempestiva à sociedade.

2. TERMOS E DEFINIÇÕES

Para fins deste documento, consideram-se os seguintes termos e definições:

• Apetite a Risco

Nível de risco, em sentindo mais abrangente, que a organização se dispõe a aceitar na busca por agregar valor aos serviços prestados para a sociedade.

• Atividades de controles internos

São as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos da SUDAM.

• Avaliação de risco

Processo de identificação e análise de riscos relevantes para alcance dos objetivos da SUDAM e a determinação de resposta apropriada.

• Categoria de Riscos

As 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 objetivos. Resulta da junção das fontes de risco com as vulnerabilidades.

• Consequência

Impacto de um evento que afeta os objetivos.

• Contexto

Diz respeito à definição dos parâmetros externos e internos e dos critérios de risco a serem levados em consideração no gerenciamento de riscos.

• Controle

Medida aplicada para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados.

• Controle Interno 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, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os objetivos gerais serão alcançados.

• Escopo

É a soma dos produtos do processo de trabalho e seus requisitos ou características.

• 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.

• Gestão de riscos

Arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente.

• Gerenciamento de risco

Conjunto de processos adotados para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável ao alcance dos objetivos organizacionais.

• Gestão de integridade

Conjunto de medidas de prevenção de possíveis desvios na entrega dos resultados esperados pela sociedade.

• Governança: combinação de processos e estruturas implantadas pela alta administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos.

• Governança pública: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade.

• 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 o reconhecimento 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

Consequência da ocorrência de um evento, podendo ocasionar mudança adversa ou positiva no alcance dos objetivos.

• Incerteza

Incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

• Medida de controle

Medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.

• Meta

Alvo ou propósito com que se define um objetivo a ser alcançado.

• Método de priorização de processos

Classificação de processos baseadas em avaliação qualitativa e quantitativa, visando o estabelecimento de prazos e demais condições para a realização de gerenciamento de riscos.

• Monitoramento

É um componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo.

• Objetivo organizacional

Situação que se 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 administrativas, 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 ricos, bem como prestar apoio às atividades de controle externo, exercidas pelo TCU.

• Plano de Controle

Registro de ações de tratamento a serem adotadas em resposta aos riscos avaliados.

• Plano de Integridade

Documento que contém o conjunto de medidas para prevenir, detectar e remediar riscos para a integridade no âmbito da Sudam. Estabelece o compromisso da alta administração e das unidades, sendo um importante documento de divulgação e disseminação da cultura de integridade dentro e fora da organização.

• Política de gestão de riscos:

Declaração das intenções e diretrizes gerais relacionadas à gestão de riscos no âmbito da SUDAM.

• Portfólio de Riscos Prioritários

Grupo de riscos com impacto potencialmente elevado para o negócio. Deve ter a gestão priorizada e os controles monitorados regularmente.

• Processo

Conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.

• Processo de Gestão de Riscos

Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de estabelecimento do contexto, identificação, análise, avaliação, tratamento, comunicação e monitoramento.

• Processo de Trabalho

Conjunto de atividades interdependentes, ordenadas no tempo e no espaço de forma encadeada, que possuem um objetivo, início e fim, entradas e saídas bem definidas, ou comportamentos executados para alcançar uma ou mais metas.

• Proprietário do risco

Pessoa ou setor com a responsabilidade e a autoridade para gerenciar o risco.

• Probabilidade

Possibilidade de ocorrência de um evento.

• Resposta a risco

Ação adotada para lidar com risco. As respostas podem se enquadrar num destes tipos: aceitar o risco por uma escolha consciente; transferir/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/reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências.

• Risco

Possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização, sendo medido em termos de probabilidade e impacto.

• Risco Inerente

Risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir ou aumentar a probabilidade de sua ocorrência ou seu impacto.

• Risco Residual

Risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

• Tolerância a Riscos

Refere-se à variação aceitável relativa à realização de um objetivo.

• Vulnerabilidade

Ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.

3. CONDIÇÕES GERAIS

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 do 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, e o fortalecimento das ações de integridade.

A Gestão de Riscos deve apoiar de forma decisiva as ações que permitirão à SUDAM cumprir sua missão, visão, negócio e valores consignados no Planejamento Estratégico, assim compreendidos:

Missão: promover o desenvolvimento includente e sustentável da Amazônia Legal, por meio do planejamento, articulação e fomento, contribuindo para a redução das desigualdades regionais;

Visão: ser instituição de excelência em planejamento, articulação e fomento do desenvolvimento includente e sustentável da Amazônia Legal;

Negócio: desenvolvimento regional; e

Valores: comprometimento, ética e transparência, responsabilidade social e ambiental, valorização de pessoas.

4. PRINCÍPIOS E OBJETIVOS DA POLÍTICA DE GOVERNANÇA, INTEGRIDADE, RISCOS E CONTROLES INTERNOS DA SUDAM

Os princípios e objetivos da Política de Gestão de Integridade, Riscos e Controles Internos estão dispostos nos quadros 1 e 2, respectivamente:

Quadro 1 - Princípios da Governança, Integridade, Riscos e Controles Internos

1. Aderência à integridade e aos valores éticos
2. Capacidade de Resposta
3. Concepção e proteção de valores institucionais
4. Integração a todos os processos organizacionais
5. Subsídio e auxílio aos tomadores de decisão

6. Alinhamento ao contexto interno e externo da organização
7. Melhoria contínua da organização
8. Adequado suporte de tecnologia da informação para apoiar os processos de integridade, riscos e a implementação dos controles internos da gestão
9. Definição à alta administração do compromisso de atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos institucionais
10. Definição dos objetivos estratégicos que possibilitam a eficaz gestão de riscos e controles da gestão
11. Gestão sistemática, estruturada, oportuna e documentada, subordinada ao interesse público
12. Estruturação do conhecimento e das atividades em metodologias, normas, manuais e procedimentos
13. Utilização dos resultados da gestão para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de integridade, riscos e dos controles internos da gestão
14. Disseminação de informações necessárias ao fortalecimento da cultura e da valorização da gestão de integridade, riscos e controles internos da gestão
15. Realização de avaliações periódicas para verificar a eficácia da gestão de integridade, riscos e dos controles internos, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive a alta administração
16. Gestão de integridade, riscos e controles internos da gestão suportada por níveis adequados de exposição a riscos
17. Integração da gestão de integridade, riscos e controles internos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização
18. Aderência aos métodos e modelos de gerenciamento de riscos às exigências regulatórias
19. Transparência e participação
20. Prestação de contas e responsabilidade

Quadro 2 - Objetivos da Gestão de Riscos

1. Suportar a missão, a continuidade e a sustentabilidade institucional
2. Proporcionar a eficiência, a eficácia e a efetividade operacional
3. Produzir informações íntegras e confiáveis à tomada de decisões
4. Assegurar a conformidade com as leis e regulamentos aplicáveis
5. Salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida
6. Aumentar a probabilidade de alcance dos objetivos institucionais
7. Estimular a cultura da melhoria contínua dos processos organizacionais
8. Orientar os processos de gestão de riscos

5. RESPONSABILIDADES

As responsabilidades específicas para as atividades da gestão de riscos poderãos ser distribuídas em uma matriz RACI (Responsável, Responsabilizado, Consultado, Informado).

5.1. O **Comitê de Governança, Integridade, Riscos e Controles** é responsável por:

• Promover práticas e princípios de conduta e padrões de comportamentos;

• Institucionalizar estruturas adequadas de governança, gestão de integridade, riscos e controles internos;

• Promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de integridade, riscos e controles internos;

• Garantir a aderência às medidas, mecanismos e práticas organizacionais de governança, por meio de regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de contas, na transparência e na efetividades das informações;

• Promover a integração dos agentes responsáveis pela governança, pela gestão de integridade, riscos e controles internos;

• Incentivar e promover iniciativas que busquem implementar o acompanhamento de resultados institucionais, que promovam soluções para melhoria do desempenho ou que adotem instrumentos para o aprimoramento do processo decisório

• Supervisionar o mapeamento e avaliação dos riscos chave que podem comprometer a prestação de serviços de interesse público;

• Supervisionar a institucionalização e a operacionalização da gestão de integridade, riscos e dos controles internos, oferecendo suporte necessário;

• Estabelecer limites de exposição a riscos, bem como os limites de alçada ao nível de unidade, processos ou atividades;

• Aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de integridade, riscos e implementação dos controles internos da gestão;

• Emitir recomendação para o aprimoramento da governança, da gestão de integridade, riscos e controles interno;

• Monitorar a execução das recomendações deliberadas por este comitê; e

• Praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas atividades.

5.2. Cabe ao **Núcleo de Governança, Riscos e Controles**:

• Auxiliar a alta administração na implementação e na manutenção de processos, estruturas e mecanismos adequados a incorporação dos princípios e das diretrizes da governança;

• Acompanhar o tratamento dos riscos identificados;

• Propor recursos necessários às ações do comitê;

• Coordenar as atividades deliberadas pelo comitê e o tratamento dos riscos mapeados pelos gestores responsáveis das unidades administrativas;

• Realizar e acompanhar estudos de novas metodologias e tecnologias quanto a possíveis impactos na governança, integridade, riscos e controles;

• Propor normas relativas à governança, integridade, riscos e controles ou suas revisões;

• Apoiar tecnicamente as reuniões e demais atividades do comitê, incluindo o acompanhamento da execução de suas deliberações;

• Propor reuniões ordinárias ou extraordinárias do comitê;

• Solicitar assessoria técnica e informações às unidades da Sudam para subsidiar análises e decisões do CGIRC;

• Prestar orientação técnica às unidades administrativas da Sudam sobre os temas de governança, integridade, riscos e controles internos da gestão;

• Atuar como facilitador na integração dos responsáveis pela gestão de integridade, riscos e controles internos de gestão;

• Coordenar e acompanhar todas as fases do processo de gestão de riscos; e

• Exercer outras atribuições que lhe forem determinadas pelo Comitê.

5.3. Cabe aos **Gestores de Riscos** (superintendente, diretores, chefes de gabinete, coordenadores-gerais, ouvidor, coordenadores, assessores, chefes de divisão, chefes de serviço e os responsáveis pelos processos de trabalho, projetos e ações desenvolvidos) a responsabilidade de:

• Assegurar que o risco seja gerenciado e monitorado de acordo com a Política de Governança, Integridade, Riscos e Controles Internos da Sudam;

• Garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados; e

• Garantir que as informações sobre os riscos estejam disponíveis em todos os níveis da instituição.

5.4 Cabe à **Unidade de Gestão da Integridade**:

• Coordenar a elaboração e revisão do Plano de Integridade, com vistas à prevenção e à mitigação de vulnerabilidades eventualmente identificadas;

• Coordenar a implementação do programa de integridade e exercer o monitoramento contínuo, visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência de atos lesivos;

• Atuar na orientação e treinamento dos servidores da Sudam com relação aos temas atinentes ao programa de integridade;

• Promover outras ações relacionadas à gestão da integridade, em conjunto com as demais áreas da Sudam.

5.5. **Linhas ou camadas de defesa da organização**

Para coordenar os papéis dos atores envolvidos na Gestão de Integridade, Riscos e Controles Internos, a IN CGU/MP n°01/2016 apresenta a estrutura de três linhas de defesa, conforme proposto pelo *The Institute of Internal Auditors* (IIA):

1ª linha de defesa: controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, nos macroprocessos finalísticos e de apoio.

Na Sudam, a 1ª linha de defesa da Gestão de Integridade, Riscos e Controles Internos é composta pelos servidores e pelos responsáveis pelo gerenciamento de riscos dos processos organizacionais em suas respectivas unidades.

2ª linha de defesa: 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, Integridade, Riscos e Controles - CGIRC, o Núcleo de Governança, Riscos e Controles - NGRC e a Unidade de Gestão da Integridade-UGI.

O CGIRC é o órgão colegiado de decisão máxima na estrutura de governança da Sudam, constituído pelo Superintendente, que o preside, e dos titulares da Diretoria de Administração (DIRAD); Diretoria de Gestão de Fundos, de Incentivos e de Atração de Investimentos (DGFAI); e da Diretoria de Planejamento e Articulação de Políticas (DPLAN).

O NGRC é responsável pelo apoio técnico, de forma permanente, ao Comitê e às unidades administrativas da Sudam durante todas as fases de gestão de riscos e controles.

3ª linha de defesa: corresponde às auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis 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 Sudam 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.

6. PROCESSO DE GESTÃO DE RISCOS

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: análise de ambiente e fixação de objetivos; identificação dos riscos; avaliação de riscos e controles; tratamento dos riscos; monitoramento e análise crítica; comunicação e consulta; e controle e avaliação.

6.1 Sistema Agatha

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 da Administração Pública interessados.

Foi adotado pela Sudam no exercício de 2018 e seus desdobramentos de fases da gestão de integridade, riscos e controles internos serão realizadas por meio deste, o qual será complementado com Relatório semestral.

O Relatório semestral auxiliará as unidades no acompanhamento do desempenho do plano de controle e deverá ser encaminhado às partes interessadas: CGIRC, NGRC, Chefia da Unidade, Diretoria, contendo as seguintes seções:

a) Introdução;

b) Estrutura Organizacional da unidade;

c) Processos avaliados na unidade;

d) Período de avaliação;

e) Riscos identificados;

f) Avaliação dos Controles;

g) Ações de controle propostas;

h) Considerações Finais; e

i) 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.

6.2 Tipologia de Riscos

O processo de gestão de riscos adotará as seguintes categorizações de riscos:

• Estratégico:

Eventos com probabilidade de impactar na missão, nas metas ou nos objetivos estratégicos da organização;

• Risco de imagem e de reputação

Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade da SUDAM em cumprir sua missão institucional.

• Riscos à Integridade:

Eventos relacionados à corrupção, fraudes e irregularidades e/ou desvios éticos e de conduta que possam comprometer os valores preconizados pela instituição e a realização de seus objetivos.

• Operacional: eventos que podem comprometer as atividades da SUDAM, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, com impactos na eficácia e na eficiência dos processos organizacionais;

• Orçamentário/financeiro: eventos que podem comprometer a capacidade da autarquia de contar com os recursos orçamentários necessários à realização de suas atividades, ou comprometer a própria execução orçamentária, como atrasos ou antecipações no cronograma de licitações;

• Legal: decorrem de alterações legislativas e normativas que podem comprometer as atividades da SUDAM.

• Fiscal: eventos que podem afetar o equilíbrio das contas públicas;

• Integridade: eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela CGU e a realização de seus objetivos.

• Patrimonial: provocam perdas nos ativos tangíveis e intangíveis da organização;

• Tecnologia da informação: ameaças que exploram vulnerabilidades nos ativos informacionais; e

• Conformidade: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis.

7. METODOLOGIA DA GESTÃO DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS

A Metodologia de Gestão de Riscos da SUDAM estabelece e estrutura as etapas necessárias para o gerenciamento de Riscos. As etapas, conforme previsto na Política de Governança, Integridade, Riscos e Controles da Sudam, consistem em: análise de ambiente e fixação de objetivos; identificação dos riscos; avaliação de riscos e controles internos; tratamento dos riscos; monitoramento e análise crítica; comunicação e consulta; e controle 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 Planejamento Estratégico da SUDAM.

A metodologia de gestão de riscos e controles da Sudam será detalhada em documento próprio, a ser submetido ao CGIRC para aprovação.

A metodologia da gestão de integridade está disposta no Plano de Integridade da Sudam, aprovado pelo Superintendente, por meio do Ato *Ad Referendum* n°385, de 14/11/19, devido às suas particularidades.

7.1 Análise de ambiente e fixação de objetivos

Nesta etapa serão definidos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e ao estabelecer o escopo e os critérios de risco.

A análise de ambiente tem como propósito definir os fatores, internos e externos, e os critérios dos riscos. A definição desses parametrizará a atuação das demais atividades que compõem este documento.

O contexto geral deverá ser revisado e atualizado, anualmente, com base em estudos de competência do Núcleo de Governança, Riscos e Controles.

O apetite a risco corresponde ao nível de risco, em sentido mais abrangente, que o órgão se dispõe a aceitar na busca por agregar valor aos serviços prestados para a sociedade. O apetite a risco está diretamente associado à estratégia da instituição e deve ser considerado no momento de definir as estratégias.

7.1.1 Objetivos organizacionais

Concretizados pela entrega de resultados ou serviços à sociedade, os objetivos organizacionais dos macroprocessos e dos processos de trabalho estão previstos nos documentos da organização, como estatuto, regimento, planejamento estratégico. Podem ser objetivos estratégicos e operacionais; de comunicação; e objetivos de oportunidade.

A gestão de integridade, riscos e controles internos deverá estar alinhada às diretrizes constantes do Planejamento Estratégico da Sudam quanto à identidade institucional; objetivos estratégicos; mapa estratégico; indicadores e iniciativas estratégicas.

Os objetivos estratégicos da Sudam estão distribuídos em quatro perspectivas, conforme quadro abaixo:

Quadro 3 - Objetivos Estratégicos da Sudam

Perspectiva	Objetivo
	1. Atrair e manter os investimentos privados

Sociedade	2. Estimular a expansão e melhoria da infraestrutura
	3. Fomentar as atividades e arranjos produtivos locais
	4. Aumentar a atuação em Políticas e Planos Regionais Integrados
	5. Ampliar os investimentos em P&D e fortalecer o sistema de Ciência, Tecnologia & Inovação
	6. Avaliar os resultados e impactos dos instrumentos fiscais e financeiros
Processos Internos	7. Fortalecer a articulação institucional
	8. Implementar modelo de excelência e gestão, voltado para resultados
	9. Promover a comunicação institucional de forma integrada e contínua
Infraestrutura	10. Prover soluções de tecnologia da informação
	11. Modernizar a infraestrutura física e otimizar a utilização de recursos
Aprendizado e Crescimento	12. Fortalecer e valorizar o quadro de servidores
	13. Promover o desenvolvimento de conhecimentos, habilidades e atitudes

7.2 Identificação de Riscos

Consiste na busca, reconhecimento e descrição de riscos, mediante a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.

A identificação geral dos riscos deverá ser realizada nas fases iniciais do processo de gerenciamento dos riscos, visto que sua identificação em fases posteriores implicaria retrabalho e maiores custos.

O formulário para identificação dos riscos será proposto pelo Núcleo de Governança, Riscos e Controles Internos ao Comitê de Governança, Integridade, Riscos e Controles, após estudo, podendo sugerir a utilização de uma ou a combinação de mais de uma das seguintes técnicas:

• ***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, relativas aos ambientes interno e externo, geralmente apresentadas em forma de quadrantes.

• **Análise *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.

• **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.

7.3 Avaliação de Riscos e Controles

7.3.1 Análise

Refere-se à compreensão da natureza do risco e à determinação do respectivo nível de risco mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis.

• A análise de riscos fornece subsídios para as estratégias, métodos e decisões de tratamento dos riscos.

• Envolve a apreciação das causas e das fontes de riscos, suas consequências negativas ou positivas, e a probabilidade de que os eventos de riscos venham a ocorrer.

• Identifica os fatores que afetam as consequências e a probabilidade de ocorrência e os impactos dos riscos, ou a combinação de ambos, confrontado com os controles existentes, a fim de testar a eficácia e a eficiência desses controles.

• A combinação de probabilidades de ocorrência e impactos determina o nível de risco.

• Por conta da interdependência dos diversos riscos e das suas fontes, a análise de riscos poderá ser realizada em diferentes níveis de detalhe, dependendo do risco, da finalidade da análise, das informações, dos dados e dos recursos disponíveis.

• Serão utilizadas escalas para estimar a probabilidade e o impacto, conforme tabelas 1 e 2.

Tabela 1 - Escala de Probabilidade

Probabilidade	Descrição	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 cirscunstâncias pouco indicam essa possibilidade, pois não há histórico de ocorrências	2
Moderada	Possível. 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

Tabela 2 - Escala de Impacto

Impacto	Descrição	Peso
Muito Baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade)	1
Baixo	Pequeno impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade)	2
Moderado	Moderado impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade)	3
Alto	Significativo impacto nos objetivo (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade)	4
Muito Alto	Catastrófico impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade)	5

7.3.2 Avaliação

Nesta etapa são comparados os níveis de riscos com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o nível é aceitável ou se algum tratamento é exigido. Significa relacionar o grau de risco com o apetite ao risco definido pela organização, de modo a estabelecer a adequada resposta ao risco.

• A avaliação de riscos utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais destes necessitam ser tratados e quais terão prioridade no tratamento.

• A avaliação deve considerar a probabilidade de ocorrência, bem como o impacto sobre os objetivos. Quanto maior a probabilidade e o impacto, maior será o nível do risco.

A Matriz de Risco representa os possíveis resultados da combinação das escalas de probabilidade e impacto.

Tabela 3 - Matriz de Riscos

IMPACTO						
	Crítico 5	5 RM	10 RA	15 RC	20 RC	25 RC
	Alto 4	4 RM	8 RA	12 RA	16 RC	20 RC
	Moderado 3	3 RB	6 RM	9 RA	12 RA	15 RC
	Baixo 2	2 RB	4 RM	6 RM	8 RA	10 RA
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RM	5 RM
		Muito Baixa 1	**Baixa 2**	**Moderada 3**	**Alta 4**	**Muito Alta 5**
		PROBABILIDADE				

Em seguida, deve-se avaliar a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional.

O quadro abaixo demonstra os níveis de avaliação da eficácia dos controles até então existentes na SUDAM.

Quadro 4 - Níveis de Avaliação dos Controles Internos Existentes

Nível	Descrição	Fator de Avaliação dos Controles
Inexistente	Controles inexistentes mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	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.	2
Mediano	Controles implementados reduzem alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	3
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, reduzem o risco satisfatoriamente.	4
Robusto	Controles implementados são considerados adequados, e mitigam todos os aspectos relevantes do risco.	5

7.3.3 Priorização dos Riscos

Nesta etapa, devem ser considerados os valores dos níveis de riscos calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento. A faixa de classificação do risco deve ser considerada para a definição da atitude da SUDAM em relação à priorização para tratamento. O quadro 5 mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 5 - Atitude perante o risco

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 tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	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 tratamento, essa priorização deve ser justificada pela unidade e aprovada pela instância competente.

Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas está sujeita a autorização do dirigente máximo.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Crítico	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica (seção 4.11), comunicado ao CGIRC e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do CGIRC	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo CGIRC.

7.4 Tratamento de Riscos

Esta etapa objetiva definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa anterior. Desse modo, a organização deverá selecionar uma ou mais opções de tratamento para cada risco priorizado.

As opções de tratamento de riscos são:

• **Mitigar**: reduzir o impacto ou a probabilidade de ocorrência do risco.

• **Compartilhar**: compartilhar ou transferir uma parte do risco a terceiros.

• **Evitar**: ação para evitar totalmente o risco.

• **Aceitar**: aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.

O quadro abaixo apresenta descrição das modalidades de tratamento ou resposta aos riscos, fazendo correlação com os diferentes níveis de risco: baixo, moderado, alto, crítico.

Quadro 6 - Modalidades de tratamento de risco

Opção de tratamento	**Descrição**
Mitigar (ou reduzir)	Normalmente o risco é mitigado quando classificado como “Alto” ou “Extremo”. A implementação de controles apresenta um custo/benefício adequado. Neste caso devem ser implementados controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Um risco normalmente é compartilhado, ou transferido, quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Um exemplo clássico de compartilhamento do risco é a contratação de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Significa encerrar, ou descontinuar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Governança, Integridade, Riscos e Controles.
Aceitar	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

7.4.1 Plano de Controle

O Plano de Controle deve apresentar as medidas de tratamento dos riscos desse processo organizacional:

• 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;

• Data da conclusão: informar data prevista para a conclusão.

Os controles internos da gestão, adotados para mitigar riscos, podem ser classificados como preventivos, corretivos, diretivos ou de detecção:

• Revisões da Alta Administração;

• Revisão de superiores;

• Normatizações internas;

• Autorizações e aprovações;

• Controles físicos;

• Segregação de funções;

• Capacitação e treinamento;

• Verificações;

• Conciliações;

• Indicadores de desempenho; e

• Revisão de desempenho operacional.

No sistema Agatha é realizado o acompanhamento do plano de controle durante sua execução, podendo ser incluído, para cada ação novo acompanhamento, informando-se o status do plano de ação (a iniciar, iniciado, concluída ou cancelada), se o controle foi implementado como planejado (sim, não ou parcialmente), e as justificativas/ações realizadas ou observações. Também é possível inserir anexos na tela.

7.4.2 Validação das etapas do gerenciamento de riscos

Os resultados das etapas anteriores do processo de gerenciamento de riscos devem ser avaliados e aprovados pelo Comitê de Governança, Integridade, Riscos e Controles.

Após aprovação, o CGIRC encaminhará esses resultados ao Núcleo de Governança, Riscos e Controles que fará apresentação ao dirigente máximo da unidade organizacional.

O dirigente da unidade organizacional negociará com os gestores de riscos da sua área, a definição e a implementação de Plano de Controle que deve contemplar as estratégias de resposta aos riscos.

7.4.3 Implementação do Plano de Controle

A implementação do Plano de Controle envolve a participação da unidade organizacional responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas no Plano.

A responsabilidade primária pelas ações constantes do Plano de Controle permanece com a unidade organizacional responsável pelo processo organizacional. Neste plano, deve ser definido o principal responsável pela implementação da iniciativa (servidor ou cargo), que também deverá monitorar e reportar a evolução das iniciativas.

7.5 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.

Com base no monitoramento serão elaborados os Relatórios Semestrais, os quais serão encaminhados pelas unidades à sua Chefia, Diretoria ou Superintendente, CGIRC e ao NGRC. Caso sejam identificadas deficiências ou vulnerabilidades, serão feitas recomendações por estas instâncias para aperfeiçoamento dos instrumentos de gestão de integridade, riscos e controles.

Outra importante ferramenta de apoio a ser utilizada é a Matriz de Responsabilidade RACI, pois define Responsável, Autoridade, Consultado, Informado, em relação ao processo de gerenciamento de riscos:

• Responsável: quem executa a atividade;

• Autoridade: quem aprova a tarefa ou produto, podendo delegar a função, mas mantém a responsabilidade;

• Consultado: quem pode agregar valor ou é essencial para a implementação;

• Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Quadro 7 - RACI para atividades de Gestão de Riscos

	CGIRC	NGRC	Superintendente	Responsável pelo gerenciamento de riscos	Equipe Técnica	Responsável pela implementação	Demais servidores
Definir Plano de Gestão de Riscos	A	I	R	C	I	I	I
Selecionar processo organizacional	A	C	R	C	I	N/A	N/A
Realizar entendimento do contexto	I	C	A	R	R	N/A	N/A
Identificar e analisar riscos	I	C	A	R	R	N/A	N/A
Avaliar riscos	I	C	A	R	R	N/A	N/A
Priorizar riscos	I	C	A	R	R	N/A	N/A
Definir respostas aos riscos	I	C	A	R	R	N/A	N/A
Validar riscos levantados	I	C	R	C	C	N/A	N/A
Implementar Plano de controle	I	C	A	I	C	R	N/A
Monitorar	I/R	C	A	R	I	C	R
Realizar avaliação estratégica	A	R	C	C	R	N/A	N/A

R - Responsável; A - Aprovador; C - Consultado; I - Informado; N/A - Não se aplica.

Eventuais mudanças identificadas durante o monitoramento devem ser encaminhadas ao Núcleo de Governança, Riscos e Controles, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos.

7.6 Comunicação e Consulta

O acesso a informações confiáveis, íntegras e tempestivas é vital para o gerenciamento de integridade, riscos e controles internos.

Todos os atos relativos à governança, riscos e controles originários do CGIRC e do NGRC serão registrados no Sistema Eletrônico de Informações – SEI.

Todas as informações do gerenciamento de riscos dos processos deverão estar registradas no Sistema de Gestão de Riscos – Agatha, conforme o cronograma de implementação de gestão de riscos e de acordo com os processos priorizados para tal.

Este Plano terá validade até 31 de dezembro de 2020 e suas revisões ocorrerão a partir do exercício de 2021 de acordo com o ciclo do Planejamento Estratégico da Sudam ou quando identificada a necessidade pelo CGIRC.

O Núcleo de Governança, Riscos e Controles comunicará periodicamente o resultado do acompanhamento das ações relacionadas ao Plano de Governança, Riscos e Controles Internos, que será apresentado ao Comitê de Governança, Integridade, Riscos e Controles.

7.7 Controle e Avaliação

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.

8. INSTRUMENTOS DA GOVERNANÇA, DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS

Os instrumentos da gestão de riscos na Sudam compõem-se de:

- Política de Governança, Integridade, Riscos e Controles Internos;
- Plano de Governança, Riscos e Controles Internos;
- Plano de Integridade;
- Solução Tecnológica;
- Plano Diretor de Tecnologia da Informação e Comunicação;
- Manuais, cujos objetivos prioritários são fornecer diretrizes, princípios, orientações e operacionalização da Governança, Integridade, Riscos e Controles; e
- Metodologia, a ser detalhada em documento próprio.