MINISTÉRIO DE MINAS E ENERGIA / SECRETARIA DE GEOLOGIA, MINERAÇÃO E TRANSFORMAÇÃO MINERAL / SERVIÇO GEOLÓGICO DO BRASIL – CPRM	GOVERNANÇA	AAS 09.03
Assunto: **Gestão de Riscos Corporativos e Controles Internos**	Aprovação: **ATA DE nº 1339, de 28 de fevereiro de 2024.**	Vigência: **01/03/2024**

NORMA INTERNA

1. **FINALIDADE**

1.1. Esta norma tem por finalidade estabelecer as regras que norteiam as atividades de Gestão de Riscos e Controles Internos na Companhia de Pesquisa de Recursos Minerais (CPRM).

2. **DISPOSIÇÕES INICIAIS**

2.1. As áreas de Gestão de Riscos e de Controles Internos compõem o Departamento de Governança, integrante da estrutura da Presidência (PR) e liderada por Diretor Estatutário, que pode ser representado pelo Diretor Presidente ou outro Diretor de uma respectivas diretorias previstas no Estatuto da CPRM .

2.2. O gerenciamento de riscos é iterativo e auxilia as organizações no estabelecimento de estratégias, no alcance dos objetivos e na tomada de decisões fundamentadas.

2.3. A área de Controles Internos atua orientando o regramento de procedimentos, identificando controles existentes para adequação e fortalecimento do alcance dos objetivos da CPRM, com fins de inibir ou mitigar eventuais riscos decorrentes dos negócios da Empresa.

2.4. A gestão de riscos corporativos e de controles internos da CPRM é uma atribuição exclusiva da área da Governança, e constitui no conjunto de procedimentos por meio dos quais a empresa identifica, avalia, trata, comunica e monitora os riscos que podem afetar negativamente o alcance dos seus objetivos, conforme modelo estabelecido pela Norma Brasileira ABNT NBR ISO 31000.

2.5. A gestão de riscos corporativos e de controles internos trata-se de um instrumento que contribui para melhorar o desempenho, por meio da identificação de oportunidades e a redução da probabilidade e/ou impacto dos riscos, além de apoiar os esforços de garantia da conformidade dos agentes aos princípios éticos e às normas legais.

3. **CONCEITOS BÁSICOS**

3.1. APETITE A RISCO: quantidade de risco que a organização está disposta a aceitar para criar valor.

3.2. CONTROLES INTERNOS: ações estabelecidas por meio de instrumentos formais de procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos.

3.3. EVENTO: um ou mais incidentes ou ocorrências, provenientes do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

3.4. GERENCIAMENTO DE RISCOS: é a cultura, os recursos e as práticas que as organizações integram com a estratégia definida e executada, com o objetivo de gerenciar o risco na criação, preservação e valorização.

3.5. GESTOR DE RISCO: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco.

3.6. IMPACTO: efeito resultante da ocorrência do evento.

3.7. INSTRUMENTOS FORMAIS: documentos internos balizadores que regulamentam ou instruem à gestão nas ações necessárias para o estabelecimento da conformidade: políticas, regulamentos, regimentos, normas e instruções.

3.8. NÍVEL DE RISCO: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos.

3.9. PROBABILIDADE: possibilidade da ocorrência de um evento.

3.10. RESPOSTA AO RISCO: estratégia a ser adotada frente ao evento de risco, considerando o nível de exposição a riscos previamente estabelecido e relacionado com a avaliação que se fez na matriz de apetite a riscos.

3.11. RISCO: efeito das incertezas sobre a realização dos objetivos.

3.12. RISCO INERENTE: risco natural, ausência de qualquer ação que a direção possa realizar para alterar a probabilidade de ocorrência ou de impacto.

3.13. RISCO RESIDUAL: resultante do processo de tomada de decisão e aplicação das melhores práticas de controles internos ou da resposta da organização ao risco.

4. COMPETÊNCIAS

4.1. Compete ao Conselho de Administração:

a) aprovação das Políticas de Gestão de Riscos e de Controles Internos e Conformidade;

b) determinar a implantação e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos corporativos a que está exposta a CPRM, inclusive os riscos relacionados à integridade das informações contábeis e financeiras, bem como os relacionados à ocorrência de corrupção e fraude;

4.2. Compete à Diretoria Executiva:

a) monitorar a sustentabilidade dos negócios, os riscos estratégicos e respectivas medidas de mitigação, elaborando relatórios gerenciais com indicadores de gestão;

b) apresentar, até a última reunião ordinária do Conselho de Administração do ano anterior, Plano de Negócios para o exercício anual seguinte e estratégia de longo prazo atualizada, com análise de riscos e oportunidades para, no mínimo, os próximos cinco anos;

c) manifestar-se expressamente acerca das ações a serem implementadas para correção tempestiva das deficiências de controle e de gerenciamento do risco operacional, apontadas em relatório elaborado anualmente pela Auditoria; e

d) fomentar a cultura de gestão de riscos, a cultura de gestão por processos e a integração das práticas de gestão de riscos aos negócios e aos objetivos estratégicos.

4.3. Compete ao Diretor-Presidente:

a) atuar como principal responsável pela formulação do planejamento estratégico e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão.

b) prover os recursos e soluções de tecnologia da informação necessários para uma eficiente implementação e monitoramento da Política da Gestão de Riscos de forma integrada ao Planejamento Estratégico da CPRM.

4.4. Compete ao Comitê de Auditoria:

a) auxiliar o Conselho de Administração no monitoramento da qualidade das demonstrações financeiras, da efetividade dos sistemas de controles internos, da conformidade, do gerenciamento de riscos e das auditorias interna e independente;

b) supervisionar as atividades desenvolvidas nas áreas de controle interno, de auditoria interna e de elaboração das demonstrações financeiras da CPRM; e

c) monitorar a qualidade e a integridade dos mecanismos de controle interno, das demonstrações financeiras e das informações e mediações divulgadas pela CPRM.

4.5. Compete à Auditoria Interna:

a) avaliar a adequação dos controles internos, a efetividade do gerenciamento dos riscos corporativos e dos processos de governança, bem como a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações, visando ao preparo das demonstrações financeiras;

b) avaliar os procedimentos adotados pela empresa quanto à efetividade dos processos e controles para identificar, avaliar, monitorar e gerenciar riscos; e

c) tem por objetivo básico o exame analítico e periódico dos atos e fatos administrativos praticados nas diversas áreas da CPRM, quanto ao fiel cumprimento da Legislação, das recomendações dos Órgãos de Controle e dos Instrumentos Normativos vigentes, bem como do Orçamento e dos Programas aprovados pela Diretoria Executiva e pelo Conselho de Administração.

4.6. Compete ao Departamento de Governança:

a) propor políticas de Conformidade e Gerenciamento de Riscos para a CPRM, as quais deverão ser periodicamente revisadas e aprovadas pelo Conselho de Administração, e comunicá-las a todo o corpo funcional da organização;

b) elaboração do regimento interno de Governança;

c) elaboração das normas e instruções pertinentes à atuação do departamento de Governança;

d) coordenar os processos de identificação, classificação e avaliação dos riscos corporativos a que está sujeita a CPRM;

e) coordenar a elaboração dos planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;

f) disseminar a importância do Gerenciamento de Riscos, da Integridade, dos Controles Internos e da Conformidade, bem como a responsabilidade de cada área da CPRM nestes aspectos;

g) orientar para que haja a adequação e fortalecimento dos controles internos da CPRM e propor melhorias;

h) orientar a atuação e efetividade das áreas responsáveis por governança corporativa, conformidade, integridade corporativa, gestão de riscos e controles da CPRM e propor melhorias;

i) apoiar o Conselho de Administração na definição do limite de exposição riscos da CPRM; e

j) monitorar o mapa integrado de risco da CPRM, bem como orientar para que a gestão avalie melhorias nos planos de mitigação.

4.7. Compete aos Gestores de Riscos Corporativos:

a) assegurar que o risco seja gerenciado de acordo com a Política de Gestão de Riscos da CPRM;

b) monitorar o risco ao longo do tempo, 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 da CPRM; e

c) garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da Empresa.

5. PROCEDIMENTOS PARA A GESTÃO DE RISCOS E CONTROLES INTERNOS

5.1. Os processos devem ser iniciados, formalizados e tramitados no Sistema Eletrônico de Informações – SEI, utilizando tipo de processo “Governança: Riscos Corporativos – Matriz de Risco”. No ofício enviado pelas respectivas áreas deverá constar a Diretoria vinculada, o departamento/divisão solicitante, o processo a ser mapeado e o objetivo deste processo no contexto da CPRM.

5.2. O processo para mapeamento dos riscos corporativos poderá ser iniciado por identificação da necessidade pela própria Governança, para o cumprimento de legislação ou necessidade específica, ou por meio de demandada encaminhada pela área responsável, visando identificar e avaliar os seus riscos inerentes aos seus respectivos processos de trabalho.

5.3. No caso de solicitação externa encaminhada, a Área de Gestão de Riscos da Governança analisará o pedido para início do mapeamento dos riscos corporativos.

5.4. Em caso de não atendimento da solicitação por parte da Governança, será comunicado via SEI à área demandante a justificativa motivada da recusa.

5.5. Todos os processos de identificação e avaliação de riscos corporativos, em seus respectivos processos de trabalho na CPRM, devem ser submetidos a análise técnica da Área de Gestão de Riscos da Governança.

6. DETALHAMENTO DA METODOLOGIA DA GESTÃO DE RISCOS E CONTROLES INTERNOS

6.1. As principais etapas do modelo de gerenciamento de riscos (ISO 31.000:2018) na CPRM são:

a) estabelecimento do contexto;

b) identificação dos riscos;

c) avaliação dos riscos;

d) tratamento dos riscos;

e) comunicação dos riscos; e

f) monitoramento dos riscos.

6.2. Estabelecimento do Contexto

6.2.1. Na etapa do Estabelecimento do Contexto deve-se observar:

a) o levantamento e registro dos aspectos externos e internos ao alcance dos objetivos institucionais, permitindo a compreensão do ambiente em que a organização se insere e a identificação de fatores quem podem influenciar a capacidade da organização de atingir os resultados esperados;

b) a finalidade de colher informações para apoiar a identificação de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo;

c) a verificação, em todos os níveis da unidade, se os objetivos foram fixados e comunicados e se estão alinhados a missão e a visão da CPRM; e

d) o registro de quais etapas do processo se está avaliando, no processo de gestão de riscos.

6.3. Identificação dos Riscos Corporativos

6.3.1. Na etapa da Identificação dos Riscos deve-se observar que:

a) a identificação é de responsabilidade primária dos gestores das áreas;

b) qualquer empregado que identifique um evento que potencialize um risco deverá comunicar imediatamente ao seu gestor imediato; e

c) para a identificação dos riscos que possam afetar os objetivos devem ser considerados: a causa, o efeito/consequência e a categoria.

6.4. **Avaliação dos Riscos**

6.4.1. Na etapa da avaliação dos riscos deve-se observar que:

a) há necessidade de uma avaliação do risco inerente, dos controles existentes e, por fim, do risco residual; e

b) promover o entendimento do nível de risco, especialmente quanto à estimativa de probabilidade e do impacto dos eventos identificados.

6.4.2. Nas tabelas a seguir constam os níveis de probabilidade e impacto que devem ser observados:

I - Tabela 1 – Níveis de Probabilidade

Probabilidade	Aspectos avaliativos	Valor
Muito Baixa	Evento pode ocorrer apenas em circunstâncias excepcionais	1
Baixa	Evento pode ocorrer em algum momento	2
Média	Evento deve ocorrer em algum momento	3
Alta	Evento provavelmente ocorra na maioria das circunstâncias	4
Muito Alta	Evento esperado que ocorra na maioria das circunstâncias	5

II - Tabela 2 – Níveis de Impacto

Probabilidade	Fatores para Análise	Valor
Insignificante	Estratégico - Operacional: 1. Esforço de gestão; 2. Regulação; 3. Reputação; 4. Negócios/Serviços a Sociedade; 5. Intervenção Hierárquica. Econômico Financeiro: 1. Orçamentário/ Financeiro	1
Pequeno		2
Moderado		3
Grande		4
Catastrófico		5

III - A Multiplicação da avaliação de probabilidade e impacto forma o resultado final de avaliação de risco, o qual está inserido em quatro níveis da matriz de risco, conforme demonstrado nos quadros a seguir:

Matriz de Riscos						
Catastrófico	5	5	10	15	20	25
Grande	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Pequeno	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5

1	2	3	4	5
Muito Baixa	Baixa	Média	Alta	Muito Alta
< 10%	>=10% <= 30%	>=30% <= 50%	>=50% <= 90%	>90%

Escala de Nível de Risco	
Níveis	Pontuação
RC - Risco Crítico	13 a 25
RA - Risco Alto	7 a 12
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

6.5. **Avaliação dos Controles Internos**

6.5.1. Após a mensuração dos riscos inerentes, deve-se identificar e avaliar os controles existentes que respondam aos eventos de riscos identificados, quanto ao seu desenho e quanto à sua operação. No desenho se faz necessário identificar se há procedimento de controle suficiente e formalizado, enquanto na operação, deve-se identificar se há procedimento de controle sendo executado e se há evidências de sua execução. Todo processo de Gestão de Riscos deve observar os controles sob a ótica da relação custo-benefício, de forma a otimizar a alocação de recursos, e permitir maior alcance do valor público gerado.

6.5.2. Após análise dos controles existentes, deve-se aferir o nível de risco residual, indicando os novos pesos relativos à probabilidade e ao impacto.

6.6. **Tratamento dos Riscos e Plano de ação**

6.6.1. Conhecido o nível de risco residual, deverá ser adotada estratégia para responder ao evento de risco, que dependerá do nível de exposição a riscos previamente estabelecido, devendo as áreas de gestão de riscos e controles internos subsidiar às áreas gestoras do processo a realizar uma análise, podendo validar ou alterar a resposta ao risco, apresentando justificativa da motivação. Os quatro tipos de respostas são:

a) Evitar: não iniciar ou descontinuar a atividade que origina o risco;

b) Aceitar/Tolerar: deixar a atividade como está, não adotando qualquer medida;

c) Mitigar/Reduzir: desenvolver ações para mitigar o risco, ou seja, remover suas fontes ou reduzir a probabilidade e/ou impacto do risco; e

d) Transferir/Compartilhar: distribuir parte do risco para outros atores (terceiros).

6.6.2. Após a análise, elabora-se um Plano de Controle, que é um conjunto de ações necessárias para adequar os níveis de riscos, apontando os seguintes fatores:

a) Tipo (preventivo, corretivo ou compensatório);

b) Objetivo (adotar controle novo ou melhorar controle existentes);

c) Área responsável pela implementação;

d) Responsável pela implementação;

e) Como será implementado;

f) Intervenientes; e

g) Data do início e da conclusão.

6.7. **Comunicação dos riscos, controles e conformidade**

6.7.1. O Departamento de Governança deverá formalizar para á área envolvida via SEI, o relatório final e o mapa de gerenciamento de riscos finalizado, fornecendo acesso a informações confiáveis, íntegras e tempestivas, contribuindo para que a gestão de integridade, riscos e controles internos seja eficaz no alcance dos objetivos.

6.7.2. Além da área responsável, a Governança deverá comunicar os riscos identificados ao Conselho de Administração, Conselho Fiscal, Comitê de Auditoria Estatutário e a Diretoria Executiva.

6.8. Monitoramento dos riscos e controles

6.8.1. Deverá ser realizado ciclos de avaliação e revisões independentes, de modo a assegurar a eficácia do seu gerenciamento e monitoramento, podendo ocorrer a cara período de 6 (seis) meses.

6.8.2. Deve-se certificar sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos, sendo uma atividade desenvolvida ao longo do tempo.

6.8.3. O gestor responsável deverá manter a capacidade de avaliar e desenvolver planos de respostas.

6.8.4. As sugestões devem ser aplicadas e monitoradas pelos proprietários dos riscos, de forma a assegurar que as incertezas são gerenciados adequadamente e que as ações definidas para o seu tratamento estão sendo executadas.

6.8.5. A Governança se coloca à disposição para orientar todas as áreas responsáveis pelos processos indicados, com o objetivo de contribuir com a implementação e monitoramento das ações de controle necessárias para o adequado tratamento dos riscos, de forma a evitar os impactos negativos decorrentes de sua materialização.

6.8.6. Enquanto não consumada nova revisão do mapa de gerenciamento de riscos com todas as etapas da nova construção, permanecem válidas as condições estabelecidas na última análise.

7. DIVULGAÇÃO DOS MAPAS DE RISCOS CORPORATIVOS

7.1. Á área de Governança deverá divulgar, em sua página, os mapas de riscos corporativos gerados, para ciência dos colaboradores e da Alta Administração.

7.2. Deve-se dar prioridade aos riscos relevantes e os seus sistemas para monitorar e gerenciar os riscos.

8. DISPOSIÇÕES GERAIS

8.1. As atribuições da Governança estão discriminadas no seu Regimento Interno e no Estatuto Social da CPRM.

8.2. Os subprocessos desta norma devem ser conduzidos por meio de Instruções Normativas, por assunto específico, seguindo a formalização definida na Norma Interna AAS 09.01 – Elaboração de Instrumentos Normativos da CPRM.

8.3. A aprovação desta norma é de responsabilidade da Diretoria Executiva, conforme disposto na Norma Interna AAS 09.01 – Elaboração de Instrumentos Normativos da CPRM.

8.4. A declaração de apetite a riscos será revisada e aprovada pelo Conselho de Administração anualmente, ou sempre que necessário, bem como monitorada permanentemente pelos Administradores e Gestores das áreas de negócio e da Governança.

8.5. Os casos omissos ou conflituosos desta norma deverão serão direcionados à Diretoria Executiva.

8.6. Esta norma entra em vigor a partir da data de sua aprovação pela Diretoria Executiva, podendo ser revista e atualizada a qualquer tempo.

9. DISPOSIÇÕES FINAIS

9.1. Esta Norma AAS 09.03 - Gestão de Riscos Corporativos e Controles Internos, atribuída ao Processo SEI nº 48042.000270/2023-55, integra o Manual Assessoramento à Administração Superior – AAS – Módulo 09 – Governança.

9.2. O órgão gestor de Governança é responsável pelo histórico, controle e atualização desta Norma, cabendo-lhe, ainda, a sua compatibilização com os instrumentos normativos em vigor, bem como a sua publicação e divulgação no âmbito da Empresa.

Documento assinado eletronicamente

JULIANO OLIVEIRA

Chefe da Governança

De acordo.

INÁCIO CAVALCANTE MELO NETO

Diretor-Presidente

Distribuição: Geral

Chancelas:

Análise Técnica: Governança

Análise Jurídica: Consultoria Jurídica

Documento assinado eletronicamente por **JULIANO DE SOUZA OLIVEIRA**, **Chefe da Governança**, em 04/03/2024, às 15:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Inácio Cavalcante Melo Neto**, **Diretor(a)-Presidente**, em 07/03/2024, às 15:37, 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 sei.sgb.gov.br/autenticidade, informando o código verificador **1955405** e o código CRC **8AB37511**.

Referência: Processo nº 48042.000270/2023-55 SEI nº 1955405