

2018

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DA CPRM



Comitê de Governança, Riscos
Corporativos e Controles Internos – CGRC
CPRM
01/06/2018

Sumário

1. OBJETIVO GERAL	3
1.1. OBJETIVOS ESPECÍFICOS.....	3
2. APLICAÇÃO	3
3. REFERÊNCIAS	3
4. DIRETRIZES	3
5. PRINCÍPIOS	4
6. DEFINIÇÕES	5
7. RESPONSABILIDADES	6
8. PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS	6
8.1. ESTABELECIMENTO DO CONTEXTO.....	6
8.2. IDENTIFICAÇÃO DOS RISCOS.....	7
8.3. ANÁLISE DOS RISCOS.....	7
8.4. TRATAMENTO DOS RISCOS.....	7
8.5. MONITORAMENTO DOS RISCOS.....	7
8.6. COMUNICAÇÃO DOS RISCOS.....	7
9. DISPOSIÇÕES GERAIS	8

1. OBJETIVO GERAL

Orientar as atividades de avaliação, tratamento, monitoramento e comunicação dos riscos corporativos inerentes às atividades da CPRM, incorporando boas práticas de Governança Corporativa para melhoria continuada dos mecanismos de gestão e controle que visam a preservação e a geração de valor, de maneira alinhada à sua missão, visão e objetivos estratégicos, em conformidade com as regulamentações aplicáveis.

1.1 OBJETIVOS ESPECÍFICOS:

- Instituir diretrizes e competências ao gerenciamento de riscos corporativos para a identificação, avaliação, priorização, tratamento, monitoramento e comunicação;
- Promover uma linguagem comum de gerenciamento de riscos, de modo a difundir o conhecimento de gestão de risco em toda empresa;

2. APLICAÇÃO

Em todas as áreas da CPRM que participam do processo de Gestão de Riscos Corporativos.

3. REFERÊNCIAS

- Estatuto da CPRM;
- COSO 2013 (*Committee of Sponsoring Organizations of the Treadway Commission*) – *Internal Control – Integrated Framework*;
- COSO ERM (*Committee of Sponsoring Organizations of the Treadway Commission*) – *Enterprise Risk Management Framework*;
- Norma ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes;
- Norma ABNT ISO GUIA 73:2009 – Gestão de Riscos: Vocabulário;
- Instrução Normativa Conjunta MPOG/CGU nº 1, de 10/05/2016 (dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal).

4. DIRETRIZES

- Implementar a área responsável pela verificação de cumprimento de obrigações e de gestão de riscos, vinculada ao diretor presidente e conduzida por ele, ou por outro diretor estatutário, que conforme seu Estatuto, prever as atribuições da área, bem como estabelece mecanismos que assegurem atuação independente, consoante estabelecido no parágrafo 2º, artigo 9º da Lei 13.303/2016;
- A prática do gerenciamento de riscos deve considerar os aspectos quanto a missão, visão e valores da empresa, viabilizando a compreensão da gestão de riscos por todos os colaboradores;
- O Conselho de Administração e Diretoria Executiva devem promover a gestão de riscos em todos os níveis hierárquicos e áreas de atuação da

empresa, assegurar a aplicação das diretrizes e a aderência aos procedimentos de gerenciamento de riscos;

- O Conselho de Administração deve assegurar-se de que a Diretoria identifica preventivamente – por meio de um sistema de informações adequado – e lista os principais riscos aos quais a organização está exposta, além da sua probabilidade de ocorrência, a exposição financeira consolidada a esses riscos (considerando sua probabilidade de ocorrência, o impacto financeiro potencial e os aspectos intangíveis) e as medidas e os procedimentos adotados para sua prevenção ou mitigação.
- O gerenciamento de riscos deve se fazer presente em todos os processos de gestão, controles internos e auditoria interna, promovendo a identificação antecipada dos riscos e a gestão tempestiva dos mesmos;
- Os riscos identificados devem ser analisados, classificados, priorizados e monitorados;
- Definir planos de ação e contingência dos riscos, bem como realizar o seu monitoramento;
- A melhoria contínua do processo de gerenciamento de riscos deve ser promovida através de ciclos de avaliação e revisões independentes, com periodicidade anual, de modo a assegurar a eficácia do gerenciamento e do monitoramento.

5. PRINCÍPIOS

Para que boas práticas de gestão de riscos sejam implantadas de forma eficaz na CPRM, é necessário que em todos os níveis hierárquicos da empresa atendam aos princípios abaixo:

- criar valor para os objetivos da CPRM;
- ser parte integrante de todo processo organizacional da empresa;
- fazer parte das decisões, auxiliando os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação;
- explicitar as incertezas;
- prover a sistemática, estrutura e agilidade na abordagem do gerenciamento de riscos, contribuindo de forma eficiente e consistente;
- basear-se nas melhores informações disponíveis;
- alinhar a empresa ao contexto externo e interno;
- fatores culturais e humanos são levados em conta;
- processos transparentes e que incluam todas as pessoas envolvidas;
- promover respostas a mudanças de forma dinâmica e interativa;
- prover a empresa com ferramentas apropriadas continuamente.

6. DEFINIÇÕES

- Avaliação de riscos: Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável;
- Controles internos: Ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos;
- Evento: um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer;
- Gestão de riscos: atividades coordenadas para dirigir e controlar a organização no que se refere a riscos e a oportunidades. A gestão de riscos, através de um enfoque estruturado e da melhor compreensão das inter-relações entre riscos, alinha estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e a criação de valor para a organização;
- Gestor de risco: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco;
- Governança Corporativa: Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum;
- Incerteza: estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A incerteza pode se transformar em ameaça ou em oportunidade para a organização;
- Natureza de risco: – Classificação que permite a organização dos riscos em função das áreas da organização que são afetadas pelos eventos. Os riscos podem pertencer a categorias distintas e em alguns casos poderão se encaixar em mais de uma categoria concomitantemente;
- Nível do risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos;
- Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos;
- Risco: efeito das incertezas sobre a realização dos objetivos.
- Risco estratégico: definido como a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos relacionados aos objetivos de alto nível, assim entendidos, os que dão suporte e estejam alinhados à missão institucional;

- Risco operacional: estimativa das perdas diretas ou indiretas resultante de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos;
- Risco inerente: risco natural, ausência de qualquer ação que a direção possa realizar para alterar a probabilidade de ocorrência ou de impacto;
- Risco residual: resultante do processo de tomada de decisão e aplicação das melhores práticas de controles internos ou da resposta da organização ao risco.

7. RESPONSABILIDADES

- Conselho de Administração: aprovar a política;
- Presidência ou diretor estatutário: revisar e aprovar as definições gerais das estratégias de gestão de risco;
- Comitê de Governança, Riscos Corporativos e Controles Internos: realizar uma avaliação contínua da adequação e da eficácia de seu modelo de gestão de riscos, que deve ser continuamente monitorado, visando assegurar a presença e o funcionamento de todos os seus componentes ao longo do tempo;
- Coordenação de Integridade e Riscos Corporativos e Coordenação de Controles Internos:
 - ✓ Manter a diretoria e o Comitê regularmente informados sobre os riscos aos quais estão sujeitos a companhia;
 - ✓ Estabelecer procedimentos, parâmetros para gerenciar os riscos da instituição, promovendo o desenvolvimento de uma cultura de riscos e comunicação que envolva todos os colaboradores da empresa;
 - ✓ Identificar, em conjunto com as áreas, os riscos operacionais inerentes a cada um dos processos;
 - ✓ Responsável pela disseminação da cultura de controles internos da empresa;
- Áreas Operacionais: A gestão de riscos é de responsabilidade de todos, sendo que os gestores de cada área atuam como representantes do Comitê de Governança, Riscos Corporativos e Controles Internos facilitando a comunicação e a divulgação de informações ou procedimentos que sejam necessários, bem como reportando ao Comitê qualquer evento de risco que impactou ou que foi previamente detectado em sua área de atuação.

8. PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS

Em um processo de gestão de riscos podem existir várias etapas e atividades. O processo de gestão de riscos da CPRM está estruturado em 6 etapas, que são a base para os principais regulamentos de gestão de riscos, incluindo o COSO e a ISO 31000.

8.1. ESTABELECIMENTO DO CONTEXTO

Definição dos critérios para gestão de riscos e o escopo da gestão, as áreas e setores envolvidos. O contexto deve ser dividido em contexto interno e externo em relação a organização. No contexto interno a organização deve analisar sua estrutura organizacional, responsabilidades, processos, os sistemas de informação internos e o diálogo e relações com as partes interessadas internas. No contexto externo questões como o ambiente legal, social, cultural, político, financeiro, tecnológico, econômico, dentre outros devem ser avaliados, assim como a relação com partes interessadas externas, a sua percepção e seus valores.

8.2. IDENTIFICAÇÃO DOS RISCOS

Reconhece e descreve os riscos aos quais a Empresa está exposta. Nessa fase são levantados e definidos os eventos, causas, impactos e responsáveis pelos riscos.

8.3. ANÁLISE DOS RISCOS

Realiza estudos viabilizando:

- Definição dos atributos de impacto (quantitativo ou qualitativo) e probabilidade, considerando efeito dos controles já existentes (risco residual);
- Elaboração do Mapa de Riscos da CPRM, ferramenta suporte para priorização de esforços para minimização dos principais riscos, considerando apetite a risco definido pela empresa.

8.4. TRATAMENTO DOS RISCOS

Envolve a seleção de ações para responder aos riscos: evitar, mitigar, compartilhar, aumentar ou aceitar. O tipo e o nível de resposta/priorização dependem, principalmente, da materialidade, criticidade e relevância do risco, bem como do apetite ao risco que foi definido pela empresa.

8.5. MONITORAMENTO DOS RISCOS

Para o monitoramento dos riscos definidos nas etapas acima, é necessário:

- Supervisão da implantação e manutenção dos planos de ação e iniciativas previstas na fase de tratamento e o alcance das metas estabelecidas, através de atividades gerenciais contínuas e/ou avaliações independentes;
- Acompanhamento do desempenho dos indicadores de riscos;
- Aprimoramento contínuo do processo de gestão de riscos;
- Detecção de mudanças no contexto interno e externo, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos e suas prioridades;
- Identificação de riscos emergentes.

8.6. COMUNICAÇÃO DOS RISCOS

Deve ser contínua e interativa permeando todo o processo de Gestão de Riscos Corporativos.

9. DISPOSIÇÕES GERAIS

- Esta política deve ser acompanhada pelo conselho de administração e diretoria executiva da CPRM, no tange à aplicação dos procedimentos de acompanhamento e ao controle de suas diretrizes;
- A CPRM deve garantir que os princípios e diretrizes estabelecidos nesta política sejam aplicados e divulgados para todos os colaboradores da empresa;
- Quando necessário esta política deve ser desdobrada em outros documentos normativos específicos, porém sempre alinhados às diretrizes e princípios aqui estabelecidos;
- As exceções, eventuais violações e casos omissos a esta política devem ser submetidos à apreciação do Comitê de Governança, controles e Riscos Corporativos e encaminhados para posterior aprovação pelos órgãos competentes.
- Esta Política foi aprovada pela Ata nº 221 de 26 de julho de 2018.

Junho de 2018

COMPANHIA DE PESQUISA DE RECURSOS MINERAIS – CPRM

Comitê de Governança, Riscos Corporativos e Controles Internos CGRC

Conselho de Administração