COMPANHIA DE DESENVOLVIMENTO DE MINAS GERAIS

POLÍTICA CORPORATIVA

PC 10 – Política de Gestão de Riscos

REGISTRO DAS REVISÕES

Nº	Data	MOTIVO DAS REVISÕES
0	16/03/2018	Aprovação da Política
1	18/12/2018	Revisão para padronização da norma e adequação à reestruturação societária
2	11/03/2021	Revisão no item 4.1 para atualização da definição de riscos conforme norma ISO 31000; atualização das categorias de riscos; melhoria textual no documento.
3	08/11/2022	Revisão para: mudanças textuais, adequações as legislações em vigor pertinentes a esta Política Corporativa e inclusões de Políticas Internas, bem como ajustes nos itens desta política.
4	01/03/2023	Revisão da Norma: (1) Ajustes textuais, formatação e adequação de itens.

ELABORAÇÃO	VERIFICAÇÃO	APROVAÇÃO
DATA: 27/07/2023 **Gerência de Integridade, Conformidade e Gestão de Riscos**	**DATA: 31/07/2023** **ASS: _____** Misma Ferreira de Paula **Gerência de Integridade, Conformidade e Gestão de Riscos**	**DATA: xx/08/2023** **Ata da xxª Reunião do Conselho de Administração**

ESTE PROCEDIMENTO ENTRA EM VIGOR NA DATA DE SUA APROVAÇÃO.

REQUER TREINAMENTO: [ ] SIM [X] NÃO

Código: PC 10	Política de Gestão de Riscos	Vigência a partir de XX/XX/2023

SUMÁRIO

Código: PC 10	Política de Gestão de Riscos	Vigência a partir de XX/XX/2023

1. ABRANGÊNCIA

Esta política aplica-se à Codemge e suas subsidiárias. Para fins desta política, Codemge refere-se à Companhia e todas as suas subsidiárias.

2. FINALIDADE

Definir as diretrizes, conceitos e responsabilidades do processo interno de gerenciamento de riscos da Companhia, incluindo os procedimentos adequados para a identificação, categorização, avaliação, tratamento e monitoramento dos riscos atrelados aos negócios e aos objetivos estratégicos da Codemge, suas controladas e subsidiárias.

3. FUNDAMENTAÇÃO LEGAL E NORMATIVA

a) **Constituição da República Federativa do Brasil de 1988.**
b) **Constituição do Estado de Minas Gerais de 1989.**
c) **Lei nº 8.429, de 2 de junho de 1992:** Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências.
d) **Lei nº 12.846, de 1º de agosto de 2013:** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.
e) **Lei nº 13.303, de 30 de junho de 2016:** Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
f) **Lei nº 13.709, de 14 de agosto de 2018:** Lei Geral de Proteção de Dados Pessoais (LGPD).
g) **Lei nº 14.133, de 1º de abril de 2021:** Lei de Licitações e Contratos Administrativos.
h) **Decreto nº 11.129, de 11 de julho de 2022:** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.
i) **Decreto Federal nº 8.945, de 27 de dezembro de 2016:** Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
j) **Decreto Federal nº 11.129, de 12 de julho de 2022:** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.
k) **Decreto Estadual nº 46.644, de 6 de novembro de 2014:** Dispõe sobre o Código de Conduta Ética do Agente Público e da Alta Administração Estadual.

l) **Decreto Estadual nº 46.782, de 23 de junho de 2015:** Dispõe sobre o Processo Administrativo de Responsabilização, previsto na Lei Federal nº 12.846, de 1º de agosto de 2013, no âmbito da Administração Pública do Poder Executivo Estadual.

m) **Decreto Estadual nº 47.154, de 20 de fevereiro de 2017:** Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito do Estado, nos termos da Lei Federal nº 13.303/2016, e dá outras providências.

n) **COSO - ERM:** Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.

o) **ABNT NBR ISO 31000:** Gestão de Riscos: Princípios e Diretrizes.

p) **PC 01 - Política Corporativa Anticorrupção.**

q) **PC 02 - Política de Compliance.**

r) **PC 04 - Política de Segurança da Informação da Codemge.**

s) **PC 16 - Política de Privacidade da Codemge.**

t) **IN 18 – Instrução Normativa de Conduta da Codemge.**

4. DEFINIÇÕES

4.1. Aceitar o Risco: ações de retenção, redução, transferência ou exploração de determinado risco. Deve-se entender: a) como retenção, a manutenção do risco no nível atual de impacto; b) como redução, as ações para redução do nível de impacto do risco; c) como transferência, a utilização de seguros ou de eventual terceirização da atividade de risco para uma empresa de maior especialização; e d) exploração como o acréscimo do grau de exposição da Companhia ao risco, possibilitando outras vantagens competitivas.

4.2. Ambiente de Controle: conjunto de normas, processos e estruturas organizacionais para todos os componentes da estrutura de gerenciamento de riscos. O ambiente de trabalho é composto pelo: a) Estatuto Social da Companhia, seu Código de Conduta, Ética e Integridade, políticas, regulamentos e regimentos internos aprovados pelo Conselho de Administração, bem como todas as leis, regulamentos, normas, decretos e outras disposições a que a Companhia se submeta; b) práticas adotadas por cada uma das áreas da Companhia, visando a manter seus negócios operando de forma eficiente, eficaz, ética e íntegra; e c) órgãos de governança corporativa, a Diretoria, o Conselho de Administração, Comitê de Auditoria Estatutário e os empregados da Companhia.

4.3. Atividades de Controle: conjunto de atividades desenvolvidas no âmbito da Companhia visando ao gerenciamento dos riscos, incluindo: a) a revisão e aprovação das normas e procedimentos; b) a revisão e/ou aprovação de atividades, processos e serviços; c) a prévia avaliação legal ou regulatória de atividades, processos e serviços; d) o estabelecimento e aplicação de um programa de gestão de continuidade de negócios, e; e) o monitoramento de atividades, processos e serviços para controle dos riscos existentes.

4.4. Atividades de Monitoramento: atividades de mapeamento das diversas áreas da Companhia, sendo responsáveis pela detecção de novos riscos e por determinar a

efetividade dos controles implementados para os riscos conhecidos, devendo cobrir toda e qualquer operação da Companhia. Por meio das atividades de mapeamento, os riscos são identificados, categorizados e avaliados, proporcionando um mecanismo facilitador para a tomada de decisão pela área competente.

4.5. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

4.6. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa.

4.7. Evitar ou Eliminar o Risco: decisão de não se envolver com a atividade, processo ou serviço que gere determinado risco, ou agir de forma a descontinuar ou se retirar daquela atividade, processo ou serviço.

4.8. Matriz de riscos: ferramenta utilizada para registrar os riscos identificados, a avaliação de seus impactos e a probabilidade de ocorrência.

4.9. Tratamento de dados pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5. ESCOPO E DIRETRIZES GERAIS

5.1. A Codemge deve realizar o monitoramento regular dos riscos mapeados no curso normal das atividades de gestão.

5.2. O escopo, a frequência e avaliações ou revisões dos riscos mapeados variam de acordo com a avaliação do nível e criticidade dos riscos e as leituras dos indicadores de monitoramento.

6. APETITE A RISCOS E LIMITES ACEITÁVEIS PARA RISCOS

6.1. A Codemge possui perfil conservador de apetite a riscos, cujo detalhamento consta na declaração de perfil de riscos da organização.

6.2. Os limites aceitáveis para assunção de riscos, bem como as alçadas responsáveis pela aprovação deverão estar igualmente definidos na declaração.

7. RISCOS

7.1. Em atendimento ao art. 42, inciso X, da Lei nº 13.303/2016, o art. 65, IV do Decreto Estadual nº 47.154/2017 normatiza que, na preparação do processo licitatório e na contratação de obras e serviços, devem ser indicados os riscos identificados na contratação e as

responsabilidades das partes para cada situação indesejada, por meio de uma matriz de riscos.

7.2. Segundo a Norma ISO 31000, risco é o "efeito da incerteza nos objetivos". Ou seja, algo inesperado que pode ser classificado como positivo ou negativo, criando tanto ameaças quanto oportunidades. Caracterizar-se-ão como riscos o potencial de eventos ou tendências continuadas que pode afetar negativamente a realização dos objetivos da Companhia ou de suas atividades e processos, causando perdas financeiras, flutuações em receitas futuras, impacto em imagem, bem como todo e qualquer outro fator que tenha o potencial de afetar as atividades da Companhia.

7.3. Os riscos podem ser externos e internos. Riscos externos são eventos associados ao ambiente macroeconômico, político, social, natural ou setorial em que a Companhia opera, sendo imprevisíveis devido à falta de capacidade da Companhia de intervir diretamente sobre estes eventos. Por outro lado, os riscos internos são eventos originados na própria estrutura da empresa, pelas suas atividades ou colaboradores.

7.4. Os riscos aplicáveis à Companhia serão categorizados em:

a) Risco Operacional: associado às falhas, deficiências ou inadequação dos processos internos, pessoas, infraestrutura, afetando o esforço da gestão quanto à eficácia e eficiência dos processos organizacionais.

b) Risco Financeiro: pode afetar negativamente o equilíbrio das contas.

c) Risco Estratégicos: pode impactar na missão, nas metas ou nos objetivos estratégicos da Companhia.

d) Risco de Imagem: pode afetar a percepção e a confiança da sociedade em relação à capacidade da Companhia em cumprir sua missão institucional.

e) Risco de Integridade: pode impactar a probidade, transparência, cultura de ética e conduta da Companhia.

f) Risco de Conformidade: relacionado à adequação a leis, normativos, regulamentos internos.

7.5. Os riscos priorizados pela Codemge terão periodicidade de reavaliação mínima anual, ou sempre que identificada necessidade.

8. RESPONSABILIDADES

8.1. São responsáveis pela execução e acompanhamento da presente Política o Conselho de Administração, o Comitê de Auditoria Estatutário e a Diretoria da Companhia, por meio da Gerência de Integridade, Conformidade e Gestão de Riscos e da Auditoria Interna.

8.2. Competirá ao Conselho de Administração da Companhia:

a) estabelecer os limites de tolerância aos riscos que a Companhia deverá observar no exercício de suas atividades;

b) monitorar e reavaliar periodicamente os riscos estratégicos e de imagem;
c) quando solicitado pela Diretoria ou pelo Comitê de Auditoria Estatutário, avaliar a situação da Companhia em relação aos riscos categorizados no item 5.4; e
d) reavaliar, junto ao Comitê de Auditoria Estatutário, a adequação da estratégia de gerenciamento de riscos da Companhia.

8.3. Competirá à Diretoria da Companhia:

a) formular os objetivos estratégicos para implementação dos negócios aprovados pelo Conselho de Administração, dentro dos limites de tolerância aos riscos aprovados pelo mesmo;
b) identificar e categorizar os riscos mencionados no item 5.4, adotando medidas para o seu combate;
c) monitorar os riscos aos quais a Companhia está exposta;
d) executar ações de resposta aos riscos até que o risco volte a se adequar aos níveis de tolerância estabelecidos pelo Conselho de Administração da Companhia;
e) manter a adequada comunicação externa dos mecanismos de gerenciamento de riscos adotados pela Companhia;
f) consolidar o resultado do mapeamento dos riscos, avaliando sua eficácia;
g) elaborar relatórios anuais ao Comitê de Auditoria Estatutário sobre os resultados dos mapeamentos; e
h) sempre que solicitado, apresentar ao Conselho de Administração e ao Comitê de Auditoria Estatutário o mapa de riscos da Companhia e realizar o acompanhamento da implementação das respostas ao risco apontado.

8.4. A Gerência de Integridade, Conformidade e Gestão de Riscos vincula-se ao Diretor-Presidente e é liderada por ele. A Auditoria Interna vincula-se ao Conselho de Administração, por meio do Comitê de Auditoria Estatutário. São atribuições dessas áreas:

a) orientar e promover a aplicação das normas, diretrizes e procedimentos de integridade, riscos e conformidade para Companhia e suas subsidiárias;
b) coordenar a gestão da conformidade e dos controles internos necessários, incluindo os aspectos de fraude e corrupção;
c) orientar e promover a aplicação das políticas de gestão de riscos de acordo com a legislação vigente; e
d) exercer outras atribuições que lhe forem conferidas pelo Conselho de Administração.

8.5. Compete ao Comitê de Auditoria Estatutário:

a) periodicamente, supervisionar o gerenciamento dos riscos aos quais a Companhia está exposta;
b) acompanhar a implementação das ações de resposta sugeridas pelo Comitê, pelo Conselho de Administração ou pela Diretoria;
c) revisar, se necessário, a estratégia de gerenciamento de riscos da Companhia;
d) avaliar os trabalhos feitos pelo Auditor Independente.

8.6. Compete aos empregados e funcionários da Companhia:

a) executar as iniciativas da Diretoria para implementação dos objetivos estratégicos;
b) executar a atividades de controle;
c) apoiar a Diretoria na gestão de riscos, auxiliando na identificação, mapeamento e opinando em eventuais ações de resposta; e
d) executar as ações de respostas aos riscos mapeados dentro dos prazos estabelecidos.

8.7. É assegurada ao titular da Gerência de Integridade, Conformidade e Gestão de Riscos e da Auditoria Interna, no exercício de suas atribuições, a possibilidade de se reportar diretamente ao Conselho de Administração nas hipóteses do art. 9º, §4º, da Lei n.º 13.303/2016.

9. ESTRUTURA DE MONITORAMENTO

9.1. A definição dos indicadores de riscos, seu acompanhamento e avaliação serão supervisionados pelo Conselho de Administração.

9.2. O monitoramento contínuo será realizado pela Gerência de Integridade, Conformidade e Gestão de Riscos, que reportará ao Conselho:

9.2.1. Documentações relativas aos riscos corporativos;

9.2.2. Resultados de avaliações, análises e testes realizados;

9.2.3. Relatos e deficiências encontradas;

9.2.4. Eventuais níveis de ameaça ou exposição percebidos, e;

9.2.5. Oportunidades identificadas para exploração ou reforço e revisão dos controles implementados.

9.3. A Codemge adotará indicadores-chave de riscos construídos a partir de intervalos de tolerância à perda. Toda vez que o indicador estiver fora do intervalo, as áreas de monitoramento responsáveis na segunda linha de defesa e/ou auditoria interna serão alertadas para a verificação da necessidade de eventual intervenção.

10. COMUNICAÇÃO

10.1. Os processos de gerenciamento de riscos corporativos da Codemge são definidos em seus normativos internos e incorporados na estrutura organizacional.

10.2. Os papéis e atribuições de gestão de riscos estão determinados e distribuídos de forma clara e específica internamente, direcionando esforços para uma comunicação assertiva que permite que todos os envolvidos contribuam para o atingimento os objetivos organizacionais.

11. TRATAMENTO DE DADOS PESSOAIS

11.1. As atividades abrangidas por essa política serão realizadas respeitando o tratamento consciente de dados pessoais (especialmente os dados pessoais sensíveis), com observância obrigatória às disposições constantes na Lei nº 13.709/2018 (LGPD), na Política de Privacidade (PC16) e na Política de Segurança da Informação (PC04) da Codemge.

11.2. Os demais procedimentos omissos nesta política, relacionados à privacidade e à proteção de dados pessoais, deverão ser executados conforme diretrizes da Política de Privacidade e Política de Segurança da Informação da Codemge.

12. APROVAÇÃO

Esta política entra em vigor a partir da data de aprovação, revogadas as disposições em contrário.

Belo Horizonte, XX de março de 2022