



# Política de Gestão de Riscos

Versão 1

Ano 2018

# APRESENTAÇÃO

A Companhia de Tecnologia da Informação do Estado de Minas Gerais – Prodemge acredita que a transparência de ações de uma organização pública é fator determinante para uma efetiva realização de controle social.

A Lei 13.303/16 e o Decreto Estadual 47.154/17 dispõem sobre o estatuto jurídico da sociedade de economia mista e recomendam estabelecer políticas e práticas de Governança Corporativa.

A Gestão de Riscos estabelece de forma lógica e sistemática uma base confiável para a tomada de decisões e o planejamento estratégico, definindo as diretrizes norteadoras do gerenciamento do risco, que envolve atividades coordenadas para dirigir e controlar estes processos.

Dessa forma, apresentamos a Política de Gestão de Riscos para nortear a Companhia quanto ao gerenciamento de riscos.



# SUMÁRIO

---

1. OBJETIVO	4
2. PREMISSAS	4
3. APLICABILIDADE	5
4. DIRETRIZES	5
Gestão de Riscos	5
Gerenciamento de Riscos	5
Capacitação em Gestão de Riscos	6
5. PRINCIPAIS RESPONSABILIDADES	6
Conselho de Administração	6
Diretoria Executiva	6
Comitê de Auditoria Estatutário	7
Auditoria Interna	7
Comitê de Governança, Riscos e Controles Internos	7
Área de Gestão de Riscos	7
Gestor de Processos	7
Gerente Funcional	8
Empregados	8
6. VEDAÇÕES	8
7. DISPOSIÇÕES FINAIS	8
8. REFERÊNCIAS	8
9. APROVAÇÃO	9
10. VIGÊNCIA	9
GLOSSÁRIO	10

## 1. OBJETIVO

- 1.1 Estabelecer diretrizes e responsabilidades para a gestão de riscos corporativos da Companhia, visando especialmente a:
  - 1.1.1 Aumentar a probabilidade de atingimento dos objetivos estratégicos da Prodemge.
  - 1.1.2 Atentar para a necessidade de se identificar e tratar riscos em toda a organização.
  - 1.1.3 Facilitar a identificação de oportunidades e ameaças.
  - 1.1.4 Prezar pelas conformidades legal e normativa dos processos organizacionais.
  - 1.1.5 Melhorar a governança corporativa.
  - 1.1.6 Estabelecer uma base confiável para a tomada de decisão e o planejamento estratégico.
  - 1.1.7 Possibilitar a melhoria dos controles internos da gestão.
  - 1.1.8 Possibilitar a melhoria da eficácia e a eficiência operacional.
  - 1.1.9 Aumentar a capacidade da organização de se adaptar a mudanças.

## 2. PREMISSAS

- 2.1 Risco corporativo é o efeito da incerteza sobre objetivos estabelecidos, ou seja, a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos da Companhia, combinada com o impacto dessa ocorrência sobre os resultados pretendidos.
- 2.2 Esta política abrange os seguintes riscos corporativos:
  - 2.2.1 Riscos estratégicos: relacionados à estratégia da Companhia.
  - 2.2.2 Riscos operacionais: vinculados a processos internos, pessoas, infraestrutura e sistemas de informação - além dos riscos de imagem e legais;
- 2.3 A gestão de riscos é um dos mecanismos de governança e de tomada de decisão, com a finalidade de facilitar o alcance dos objetivos corporativos, e tem por base:
  - 2.3.1 Ser parte integrante dos processos organizacionais.
  - 2.3.2 Subsidiar a tomada de decisões.
  - 2.3.3 Ser sistemática, estruturada e oportuna.
  - 2.3.4 Ser baseada nas melhores informações disponíveis.
  - 2.3.5 Ser dinâmica, iterativa e capaz de reagir a mudanças.
  - 2.3.6 Possibilitar a melhoria contínua.
  - 2.3.7 Estabelecer o apetite ao risco.

- 2.4 A gestão de riscos estabelece meios para identificar, com base nos objetivos estratégicos da Companhia, eventos potencialmente capazes de afetá-los, operacionalizando-se por meio do gerenciamento de riscos que abrange atividades coordenadas para gerir os riscos corporativos presentes nos processos de trabalho da Companhia.
- 2.5 A gestão de riscos da Companhia define diretrizes norteadoras para o gerenciamento de riscos e controles internos, adotando o modelo das 3 (três) Linhas de Defesa, conforme estabelecido na Política de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão, disponível na Intranet.
- 2.6 Esta política atende as disposições da Lei Federal 13.303/16 e do Decreto Estadual 47.154/17, bem como as regras estabelecidas no Estatuto Social da Prodemge.

### **3. APLICABILIDADE**

Esta política aplica-se aos administradores, aos membros do Comitê de Auditoria Estatutário, empregados, prestadores de serviço e estagiários da Companhia.

### **4. DIRETRIZES**

#### **Gestão de Riscos**

- 4.1 A gestão de riscos deve ser contínua, sistemática, dinâmica e formalizada por meio de metodologia de gerenciamento de riscos, normas, manuais e procedimentos de acordo com as boas práticas de governança corporativa e ser integrada ao planejamento estratégico da Companhia, devendo seguir as diretrizes constantes desta política.
- 4.2 O processo de gestão de riscos deve prever mecanismos de comunicação contínua, incluindo relatórios sobre o desempenho da gestão de riscos, como parte do processo de governança.

#### **Gerenciamento de Riscos**

- 4.3 O gerenciamento de riscos na Companhia deve ser padronizado por meio de uma metodologia que contenha definições e orientações para:
  - 4.3.1 Definir a sistemática e os artefatos utilizados para o gerenciamento de riscos corporativos.
  - 4.3.2 Considerar os processos internos da Companhia, bem como a análise de contexto, compreendendo o ambiente externo e interno no qual o objeto de gerenciamento de riscos encontra-se inserido.
  - 4.3.3 Possibilitar a obtenção de informações úteis para a manutenção/eliminação dos riscos dentro de padrões definidos pela área de Gestão de Riscos.
- 4.4 A metodologia de gerenciamento de riscos deve contemplar atividades coordenadas que contribuam para dirigir e controlar processos, sendo constituído pelas etapas de identificação, análise, avaliação, tratamento, monitoramento e comunicação, com vistas a subsidiar o alcance dos objetivos da organização:
  - a) identificação: identificar as fontes de riscos, áreas de impacto, eventos e suas causas e consequências potenciais;

- b) análise: analisar as causas e as fontes de risco, suas consequências, e a probabilidade de que essas consequências possam ocorrer e seus impactos;
  - c) avaliação: comparar o nível de risco encontrado durante o processo de análise com os critérios de riscos pré-estabelecidos de acordo com o apetite a riscos da Prodemge;
  - d) tratamento: estabelecer medidas e controles a serem adotados pela Prodemge no intuito de responder aos riscos apurados na avaliação;
  - e) monitoramento: monitorar continuamente os riscos;
  - f) comunicação: integrar os envolvidos durante todo o processo, compartilhando informações junto às partes interessadas.
- 4.5 O gerenciamento de riscos deve priorizar o tratamento dos processos de acordo com as diretrizes da alta gestão.
- 4.6 Os indicadores de riscos serão estabelecidos e monitorados respeitando o ciclo dos processos, servindo de base para tomada de decisão quanto aos limites de exposição aos riscos corporativos.
- 4.7 O monitoramento de riscos deve ser realizado de forma contínua, permitindo identificar situações adversas e adotar as ações corretivas ou de contorno, minimizando impactos nos processos da organização.
- 4.8 As eventuais perdas aferidas por meio dos indicadores de monitoramento dos riscos deverão ser consolidadas para definição de ações e metas de contenção.
- 4.9 Nas atividades de planejamento, considera-se, sempre que couber, o risco como um dos critérios para seleção e priorização de iniciativas e ações.

### **Capacitação em Gestão de Riscos**

- 4.10 A capacitação em gestão de riscos deve ser aplicada continuamente para todos os administradores, gestores e empregados da Prodemge, para fortalecer a cultura organizacional nas áreas de atuação desta política.
- 4.11 Os administradores, nos termos do Decreto Estadual 47.154/17, devem participar, no mínimo anualmente, de treinamento sobre a Política de Gestão de Riscos da Prodemge.

## **5. PRINCIPAIS RESPONSABILIDADES**

### **Conselho de Administração**

- 5.1 Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Prodemge, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude, nos termos do Estatuto Social da Companhia.

### **Diretoria Executiva**

- 5.2 São responsabilidades da Diretoria Executiva relacionadas a esta política, nos termos do Estatuto Social da Companhia:
- 5.2.1 Estabelecer estruturas adequadas para o gerenciamento de integridade, riscos e controle internos da gestão em consonância com as diretrizes do Conselho de Administração.

5.2.2 Supervisionar o mapeamento e avaliação dos riscos que podem comprometer a realização dos objetivos estratégicos e a prestação de serviços de interesse público, reportando ao Conselho de Administração níveis de exposição a riscos as quais a Prodemge está sujeita.

5.2.3 Promover práticas e estabelecer princípios de conduta e padrões de comportamento a serem seguidos pelos empregados da Companhia, visando a assegurar a efetividade dos sistemas de gestão de riscos, de integridade e de controles internos implementados.

### **Comitê de Auditoria Estatutário**

5.3 Supervisionar as atividades desenvolvidas nas áreas de Auditoria Interna e de Controle Interno, avaliar e monitorar exposições de risco da Companhia e monitorar a qualidade e a integridade dos mecanismos de controle interno, das demonstrações financeiras e das informações e medições divulgadas, nos termos do Estatuto Social da Companhia.

### **Auditoria Interna**

5.4 São responsabilidades da Auditoria Interna relacionadas a esta política, nos termos do Estatuto Social da Companhia:

5.4.1 Aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança e a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações, visando ao preparo de demonstrações financeiras.

5.4.2 Assessorar o Conselho de Administração na supervisão dos sistemas de gerenciamento de integridade, riscos e controles internos.

### **Comitê de Governança, Riscos e Controles Internos**

5.5 Assessorar tecnicamente os administradores no aprimoramento da governança, no estabelecimento dos limites de exposição a riscos globais da Companhia, na elaboração e revisão de políticas, diretrizes, normas e metodologias relacionadas às boas práticas de integridade, de gerenciamento dos riscos e de melhoria dos controles internos.

### **Área de Gestão de Riscos**

5.6 Estabelecer e implementar metodologias, manuais, normas e procedimentos relativos ao gerenciamento de riscos.

5.7 Obter informações úteis não identificadas pela metodologia que representem impactos e que necessitam ser gerenciados.

5.8 Acompanhar continuamente o desempenho do gerenciamento de riscos, promovendo ações relacionadas, sempre que necessário.

5.9 Capacitar, no mínimo anualmente, os administradores sobre esta Política.

### **Gestor de Processos**

5.10 Manter controles internos eficazes, conduzindo procedimentos de respostas aos riscos, e propor, quando necessário, ações corretivas para resolver deficiências em processos e controles.

- 5.11 Colaborar na elaboração dos planos de controles dos riscos e gerenciar suas ações, avaliando periodicamente os resultados.
- 5.12 Monitorar os processos sob sua responsabilidade, de modo a garantir que as respostas adotadas aos riscos estejam em conformidade ao modelo de gerenciamento de riscos estabelecido por esta política.

### **Gerente Funcional**

- 5.13 Implementar ações corretivas para resolver deficiências em processos e controles.
- 5.14 Gerenciar os riscos dos processos de trabalho de acordo com esta política e normas correlacionadas, disponibilizando os recursos necessários para a implantação do modelo de gerenciamento de riscos estabelecido pela Política de Gerenciamento de Integridade, Riscos e Controles Internos.
- 5.15 Promover a aderência da equipe às regulamentações, às leis, aos códigos, às normas e aos padrões na condução das políticas e na prestação de serviços de interesse público.

### **Empregados**

- 5.16 Todos os empregados são responsáveis pelo gerenciamento de riscos e controles internos em seus processos de atuação.

## **6. VEDAÇÕES**

- 6.1 Nenhuma prática de gerenciamento de riscos poderá ser conduzida na Companhia sem a observância desta política e respectiva metodologia.

## **7. DISPOSIÇÕES FINAIS**

- 7.1 As políticas e documentos organizacionais devem observar e serem ajustados, no que couber, às diretrizes desta política.
- 7.2 O descumprimento desta política e seus desdobramentos normativos implicará, no que couber, em penalidades previstas na Instrução Normativa Regime Disciplinar.
- 7.3 Os casos omissos relativos à gestão de riscos devem ser tratados pela área de Integridade, Riscos e Controles Internos da Companhia.

## **8. REFERÊNCIAS**

- 8.1 Lei Federal 13.303, de 30 de junho de 2016.
- 8.2 Decreto Estadual 47.154, de 20 de fevereiro de 2017.
- 8.3 Estatuto Social da Prodemge
- 8.4 Código de Ética, Conduta e Integridade da Prodemge.
- 8.5 Política de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão.
- 8.6 *Committee of Sponsoring Organizations of the Treadway Commission – COSO.*

8.7 ABNT NBR ISO 31000:2009.

## 9. APROVAÇÃO

Aprovada pelo Conselho de Administração da Companhia, conforme Ata de Reunião de 6/9/2018.

## 10. VIGÊNCIA

A partir de 6/9/2018.

## GLOSSÁRIO

1. **Administradores:** membros do Conselho de Administração e da Diretoria Executiva.
2. **Agente público:** considera-se agente público todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, convênio, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em órgão ou entidade da Administração Pública Direta ou Indireta do Poder Executivo Estadual, inclusive os integrantes da Alta Administração do Poder Executivo Estadual.
3. **Apetite ao Risco:** Nível de risco que a Companhia está disposta a aceitar
4. **Committee of Sponsoring Organizations of the Treadway Commission – COSO (Comitê das Organizações Patrocinadoras da Comissão Treadway):** organização sem fins lucrativos, dedicada a melhoria dos relatórios financeiros, sobretudo pela aplicação da ética e efetividade na aplicação e cumprimento dos controles internos e é patrocinado pelas cinco das principais associações de classe de profissionais ligados à área financeira nos EUA. As recomendações da COSO relativas aos controles internos, bem como seu cumprimento e observância, são amplamente praticados e tidos como modelo e referência no Brasil e na maioria dos países.
5. **Conformidade:** estar em concordância com as leis e os regulamentos externos e internos.
6. **Gerente funcional:** titular de unidade da estrutura organizacional da Companhia.
7. **Gestor de processos:** responsável pelo gerenciamento de um ou mais processos identificados na Cadeia de Valor.
8. **Governança:** combinação de processos e estruturas implantadas pela alta administração para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos.
9. **Modelo de Três Linhas de Defesa:** modelo que define papéis e responsabilidades essenciais no gerenciamento de riscos e controles favorecendo sua eficácia. O modelo de Três Linhas de Defesa diferencia três grupos (ou linhas) envolvidos no gerenciamento eficaz de riscos:
  - 1ª. Linha de Defesa: Funções que gerenciam e têm propriedade sobre riscos.
  - 2ª. Linha de Defesa: Funções que supervisionam riscos.
  - 3ª. Linha de Defesa: Funções que fornecem avaliações independentes.
10. **Risco corporativo:** efeito da incerteza sobre objetivos estabelecidos, ou seja, a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos da Companhia, combinada com o impacto dessa ocorrência sobre os resultados pretendidos.