POLÍTICA DE GESTÃO DE RISCOS

EMPRESA MUNICIPAL DE DESENVOLVIMENTO DE CAMPINAS S/A

CNPJ: 44.602.720/0001-00

Aprovado na Reunião do Conselho de Administração realizada em 21/09/2021, às 10h00

(Registro na Ata da 202ª Reunião do CA)

POLÍTICA DE GESTÃO DE RISCOS

1. Objetivo

A Política de Gestão de Riscos da EMDEC (PGRE) visa estruturar as regras e princípios que serão utilizados para a identificação, análise, tratamento, monitoramento e comunicação dos riscos inerentes às suas atividades, buscando o aprimoramento dos mecanismos de controle interno, reduzindo as chances de incidência de cada risco, a redução de sua probabilidade ou ainda sua eliminação, na hipótese de ser aplicável tal medida mitigadora, permitindo o adequado cumprimento da função social da empresa e o alcance de seus objetivos estratégicos.

Busca-se ainda a plena adequação de todos os atos praticados pela EMDEC, à legislação e regras específicas estabelecidas para cada caso, para com isso evitar qualquer ilegalidade, segregação de função, conflito de interesses, reduzindo ou até mesmo eliminando a possibilidade de desvios de conduta, fraudes, combate à corrupção ou violações de diretrizes fundamentais da empresa e outras normas em todas as suas ações internas ou externas.

Por fim, com a incorporação das políticas de integridade será possível melhorar a imagem institucional da empresa e elevar a sua reputação no tocante às ações e serviços públicos desenvolvidos, tornando a empresa mais sólida e confiável na visão da sociedade.

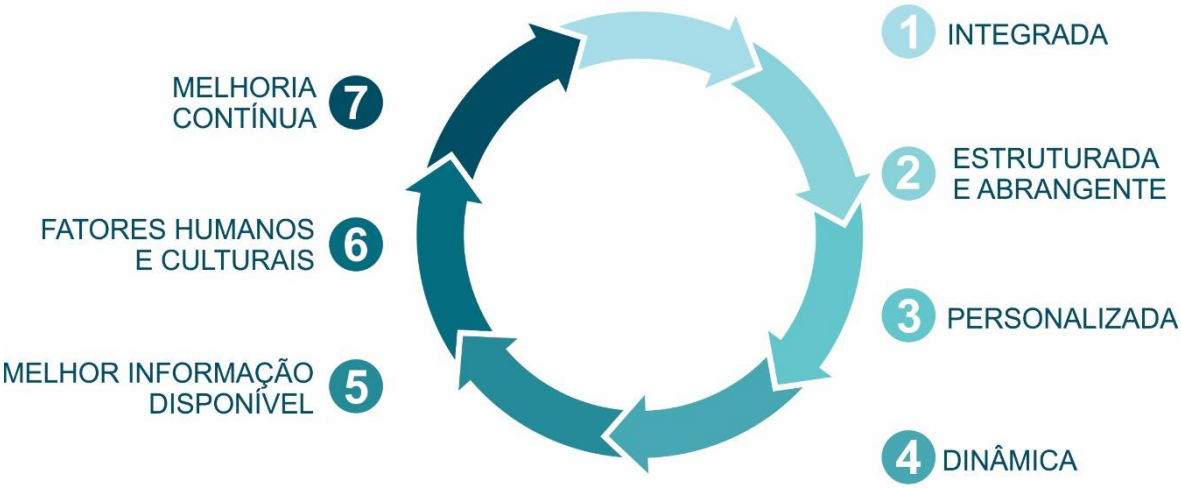

Figura 1 - Ciclo de Criação e Proteção de Valor

2. Base legal e normativa

A PGRE possui seu principal eixo na Lei Federal nº 6.404/76 que dita as normas sobre as sociedades anônimas, como também na Lei nº 13.303/2016 que determinou a obrigação legal de todas as estatais de adotarem regras específicas sobre gestão de riscos.

É importante destacar que a Lei nº 13.303/2016 em seu artigo 94 expressamente estabelece às Estatais as sanções da Lei Anticorrupção - Lei nº 12.846/2013 que prevê a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, tendo esta Lei sido um marco importante para a governança pública e privada no País.

Assim, torna-se imprescindível que as empresas estatais passem a adotar práticas de governança corporativa, para com isso evitar os riscos que são inerentes às suas atividades e que podem causar impactos de natureza financeira, legal, penal, administrativa, reputacional, dentre outros.

Dentre outros, os seguintes instrumentos legais e normativos serão considerados na PGRE:

a) Estatuto Social Consolidado da EMDEC aprovado pela A.G.O.E. de 30/04/2021;

b) Regimento Interno da EMDEC;

c) Lei Municipal nº 4.092/1972 que cria o Fundo para o desenvolvimento de Campinas, transforma o escritório municipal de planejamento em Empresa Pública - Empresa Municipal de Desenvolvimento de Campinas - Emdec, institui o plano comunitário municipal, atribui à EMDEC competência para executá-lo e dá outras providências;

d) Decreto municipal nº 4.016/1972 que transforma a Empresa Pública criada pela Lei nº 4.092, de 11 de janeiro de 1972 e denomina Empresa Municipal de Desenvolvimento de Campinas - EMDEC em sociedade de economia mista;

e) Lei Municipal nº 10.248/1999 que dispõe sobre a reorganização da Estrutura Administrativa da Prefeitura Municipal de Campinas e dá outras providências;

f) Decreto nº 19.369/2016 *que* regulamenta o estatuto jurídico das empresas públicas e de economia mista, da administração indireta do Município de Campinas;

g) Lei Municipal nº 11.263/2002 que dispõe sobre a organização dos Serviços de Transporte Público Coletivo de Passageiros no Município de Campinas e dá outras providências, e legislações regulamentadoras correlatas;

h) Código de Conduta e Integridade da EMDEC;

i) Regulamento de Licitações e Contratos da EMDEC;

j) Comunicados do Presidente, emitidos pela Presidência, que dispõe sobre a instituição de procedimentos e práticas a serem observadas na condução de matérias diversas;

k) ABNT NBR ISO 31000:2018, Gestão de riscos – Princípios e diretrizes;

l) Comunicado do Presidente nº 60/2020 – nomeação do Comitê de Conformidade e Gerenciamento de Riscos.

3. Amplitude

O estabelecimento da presente política de gestão de riscos busca definir de forma precisa o contexto organizacional da EMDEC, iniciando com a compreensão de objetivos e o comprometimento da empresa em relação à gestão de riscos para que tal política esteja alinhada a tais objetivos e demais políticas da empresa.

Por tal razão é imprescindível que a política de gestão de riscos seja parte integrante de toda a organização, tendo o apoio de seus administradores e membros das áreas que lideram os processos organizacionais.

Conclui-se assim que tal política abrange o Conselho de Administração, Comitê de Auditoria Estatutário, Diretorias, Controle Interno áreas responsáveis pelos processos de negócio prioritários na gestão de riscos.

4. Conceitos

a) **Apetite a riscos**: grau de exposição a riscos que a Companhia está disposta a aceitar para atingir seus objetivos e criar valor para seus acionistas, respeitando as partes interessadas.

b) **Compliance**: designação utilizada na prevenção e detecção de falta de conformidade com leis e regulamentações, que possa ser cometida pelos administradores, colaboradores e parceiros de negócios da Companhia.

c) **Controles**: políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.

d) **Gestão de riscos**: atividades realizadas com a finalidade de identificar, classificar, formalizar, monitorar e/ou administrar os Riscos identificados. A Gestão de Riscos deve estar alinhada aos objetivos, estratégias e negócios da Companhia.

e) **Evento**: ocorrência ou alteração em um conjunto específico de circunstâncias. Um evento pode consistir em uma ou mais ocorrências, e pode ter várias causas. Também pode consistir em não ocorrência de alguma coisa.

f) **Plano(s) de ação:** definição das ações corretivas para reduzir a exposição aos Riscos residuais, a partir da identificação das deficiências ao longo do ciclo de avaliação do ambiente de controle/Riscos.

g) **Resposta(s) ao(s) risco(s):** decisão que será tomada após a identificação do Risco inerente ou avaliação do ambiente de controle dos Riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de Controles internos da EMDEC.

h) **Key Risk Indicators** (**KRI's**): métricas que possibilitam a identificação do grau de Risco ao qual a organização está sujeita ou ao qual tem alta probabilidade de estar sujeita e que exceda o Apetite a Riscos. Funcionam como sinais de alerta, indicando as mudanças no nível de Risco da organização ou de seus negócios.

i) **Risco(s):** ameaça de eventos ou ações que possam impactar o atingimento dos objetivos da Companhia. É inerente a qualquer atividade e pode afetar os ativos, resultados, imagem/reputação, aspectos legais, regulatórios, socioambientais ou continuidade dos negócios.

j) **Responsável pelo controle**: Consiste na identificação do responsável por alertar e gerenciar determinado controle, que obrigatoriamente, deverá estar alinhado com todos os assuntos relacionados à Gestão de Riscos sob sua responsabilidade

5. Premissas

a) Estabelecer a gestão de riscos como parte da cultura empresarial da EMDEC objetivando a geração de valor para a EMDEC.

A EMDEC reconhece que a gestão integrada de riscos corporativos está diretamente relacionada ao crescimento sustentável, criação de valor e proteção do ambiente institucional, por permitir a identificação não só de ameaças, como também de oportunidades de negócio, além da tomada de decisões baseada em riscos.

b) Adotar boas práticas de governança corporativa

A EMDEC busca adotar as melhores práticas de governança corporativa quanto à gestão de riscos e às políticas e práticas antifraude e anticorrupção, com o intuito de aprimorar e manter a transparência e a qualidade das suas informações, divulgadas interna e externamente.

c) Definir uma linguagem comum sobre riscos na EMDEC

A adoção de uma linguagem padrão de gestão de riscos na empresa é essencial ao processo, possibilitando um melhor entendimento entre as partes e um processo livre de interferências.

d) Utilizar padrões e metodologias reconhecidos pelo mercado

Com um modelo baseado em metodologias e padrões formalizados, reconhecidos pelo mercado e disseminados na empresa, a gestão integrada de riscos é capaz de se adequar a estratégias, iniciativas e estruturas organizacionais, além de atender às exigências setoriais e dos órgãos reguladores e fiscalizadores.

e) Integrar os Conselhos de Administração e Fiscal, a Diretoria Executiva, o Comitê de Conformidade e Gestão de Riscos "Compliance", a Auditoria Interna, o Comitê de Auditoria Estatutário e a Controladoria Interna.

f) Estabelecer e manter a infraestrutura necessária para a gestão integrada de riscos

O gerenciamento de riscos requer uma infraestrutura adequada e integrada de processos, pessoas e tecnologia, estabelecendo mecanismos de comunicação claros e objetivos.

g) Integrar a gestão de riscos aos processos organizacionais

A gestão integrada de riscos deve permear todas as práticas e processos organizacionais da EMDEC de forma a garantir a identificação de eventos de riscos inerentes a todas as suas áreas de negócio.

h) Analisar periodicamente a gestão de riscos na EMDEC.

O Comitê de Conformidade e Gestão de Riscos "Compliance" juntamente com a Auditoria Interna, deverá assegurar a eficácia do gerenciamento de riscos por meio de monitoramento e revisões frequentes, favorecendo o cumprimento de seus objetivos

6. Metodologia

A norma ABNT NBR ISSO 31000:2018 estabelece um roteiro para que seja feita a identificação, análise, avaliação e tratamento dos riscos identificados, selecionando a opção de tratamento que melhor se adequar às características da empresa, com base nos benefícios, custos, vantagens e desvantagens de sua implementação. Destaca-se abaixo, a ilustração de como é realizado o processo de gestão de riscos, com base na ISO 31000-2018 que é "parte integrante da

gestão e da tomada de decisão, e seja integrado na estrutura, operações e processos da organização[1]":

Figura 2 - Processo de Gestão de Riscos (Adaptado da ABNT NBR ISO 31000)

Com o diagnóstico e plano de ação idealizado, será proposto pelo Comitê de Conformidade e Gerenciamento de Riscos ao Conselho de Administração da EMDEC que terá por responsabilidade aprovar ou não a implementação proposta, realizando os ajustes que forem necessários.

[1] ABNT NBR 31000-2018, p. 9

A Comissão de Conformidade e Gestão de Riscos adotará o “Modelo de Três Linhas” (anteriormente conhecido como “Modelo de Três Linhas de Defesa”) desenvolvido pelo The Institute of Internal Auditors (The IIA) e mundialmente adotado por empresas e governos. O modelo apresenta uma abordagem baseada em princípios adaptáveis aos objetivos da Organização, oferece clareza nas atribuições e relações entre as partes envolvidas e possibilita a implantação de medidas para garantir que a atividade e objetivos estejam alinhados com as normas de conformidade estabelecidas.

Figura 3 - Gráfico do Modelo de Três Linhas (Adaptado da Declaração de Posicionamento do The IIA)

Adaptando o modelo à estrutura organizacional da EMDEC, os processos proprietários de riscos juntamente com a alta Administração devem atuar como primeira linha de defesa, realizando o gerenciamento dos riscos específicos de suas atividades.

A comissão de Conformidade e Gestão de Riscos atua como segunda linha de defesa, desenvolvendo e monitorando os controles referentes à primeira linha e também sendo responsável por fornecer orientações e treinamentos e auxiliar no desenvolvimento de processos e controles para gerenciamento de riscos.

Na terceira linha encontra-se a Auditoria Interna e Comitê de Auditoria Estatutário, responsável pela avaliação geral, de forma independente e objetiva, sobre a adequação dos controles internos e efetividade da gestão de riscos.

7. Diretrizes

A EMDEC, visando alcançar os objetivos desta política, deve executar as macro etapas do processo de gestão de riscos, descritas a seguir:

7.1. Identificação dos riscos

7.1.1. A identificação de riscos deve reconhecer e descrever os riscos aos quais a empresa está exposta, considerando inclusive as possíveis alterações em seu ambiente de negócios.

7.1.2. Nesta etapa, devem ser definidos eventos, causas, consequências e responsáveis por cada risco.

7.1.3. A identificação dos riscos deve ser realizada com a participação de todos os envolvidos nos processos de negócio da empresa, nos seus diferentes níveis.

7.1.4. Os riscos identificados são categorizados de acordo com a seguinte classificação:

Tabela 1 – Categorias de risco

Negócio	Riscos inerentes aos seus processos finalísticos; à tomada de decisões; ao ambiente regulatório; aos processos que impactam na continuidade, no crescimento e no valor da empresa, e na habilidade de proteger-se ou adaptar-se a mudanças no ambiente de negócios.
Operacional	Riscos inerentes aos seus processos-meio; à eficácia e eficiência das atividades rotineiras da EMDEC; e à consistência e adequação dos sistemas de informação.
Financeiro	Riscos decorrentes de processos e atividades que envolvem as finanças e os resultados da empresa, como risco de liquidez, risco de endividamento.
Conformidade	Riscos decorrentes do não cumprimento de leis e regulamentações aplicáveis à empresa e de políticas, código de conduta e regulamentos internos.

7.2. Avaliação dos riscos

7.2.1. Após a identificação dos riscos, devem ser realizadas análises qualitativas e/ou quantitativas, visando à definição dos atributos de impacto e probabilidade, utilizados na priorização dos riscos a serem tratados.

7.2.2. A avaliação de riscos deve considerar, inclusive, o levantamento e a análise das respostas aos riscos já existentes, apurando, assim, os riscos residuais.

7.3. Tratamento dos riscos

7.3.1. Posteriormente à avaliação, a Diretoria Executiva deve definir seu posicionamento frente ao risco em comparação ao seu apetite definido pelo Conselho de Administração. As opções de posicionamento podem ser:

a) Evitar – a empresa opta por não iniciar ou não continuar em atividades que possam gerar riscos ou provocar sua exposição aos mesmos.

b) Conviver / Aceitar – a empresa entende que a exposição ao risco está de acordo com seu apetite; ou entende que o esforço para mitigá-lo ou transferi-lo seria maior do que o valor do impacto causado por sua materialização; ou, devido ao risco ser de origem externa, porém inerente às suas atividades, não tem como reduzir sua exposição. Conviver pressupõe monitorar a exposição da empresa ao risco.

c) Mitigar / Transferir – a empresa busca minimizar sua exposição ao risco, seja reduzindo o impacto e/ou a probabilidade com respostas aos riscos, ou transferindo/compartilhando os impactos do risco com outros agentes.

7.3.2. Caso o posicionamento seja evitar ou mitigar ou transferir, a EMDEC deve executar respostas de maneira que a exposição aos riscos não exceda o apetite aprovado pelo Conselho de Administração.

7.4. Monitoramento dos riscos

7.4.1. No processo de monitoramento deve-se: supervisionar a implantação e a manutenção das respostas aos riscos; verificar o alcance das metas das respostas estabelecidas por meio de atividades gerenciais contínuas e/ou avaliações independentes; garantir que as respostas

sejam assertivas, eficazes e eficientes; detectar mudanças no contexto externo e interno, identificando riscos emergentes; e analisar as mudanças nos eventos de risco, tendências, sucessos e fracassos, e aprender com eles.

7.4.2. Nas avaliações periódicas, as áreas proprietárias dos riscos devem envidar esforços em definir, adicionalmente, modelos e/ou indicadores de risco para o monitoramento de seu status e a comparação com tolerâncias e limites específicos do risco, aprovados pelo Conselho de Administração.

7.5. Comunicação dos riscos

7.5.1. A comunicação, durante todas as etapas do processo de gestão de riscos, deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado.

8. Responsabilidades

8.1. Conselho de Administração

a) Aprovar a Política de Conformidade e Gestão de Riscos conforme elaborada pela Comissão de Conformidade e Gerenciamento de Risco.
b) Implementar e supervisionar a gestão de riscos e controle interno visando a mitigação dos principais riscos elencados, sobretudo àqueles relacionados à ocorrência de corrupção e fraude e integridade de informações contábeis e financeiras.

8.2. Presidência (Diretoria)

a) Monitorar a sustentabilidade dos negócios, os riscos estratégicos e respectivas medidas de mitigação;
b) Designar os membros para a Comissão de Conformidade e Gerenciamento de Risco, composta por equipe multidisciplinar
c) Aprovar o Manual de Conformidade e Avaliação de Risco, a ser emitido pela área de Conformidade e Gerenciamento de Risco.
d) Monitorar os resultados obtidos referentes aos riscos estratégicos e respectivas medidas de mitigação.

8.3. Comissão de Conformidade e Gerenciamento de Risco

a) Propor políticas de Conformidade e Gerenciamento de Riscos para a empresa, as quais deverão ser periodicamente revisadas e aprovadas pelo Conselho de Ad-ministração, e comunicá-las a todo o corpo funcional da organização;
b) Verificar a aderência da estrutura organizacional e dos processos, produtos e serviços da empresa às leis, normativos, políticas e diretrizes internas e demais regulamentos aplicáveis;
c) Comunicar à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria a ocorrência de ato ou conduta em desacordo com as normas aplicáveis à empresa;
d) Verificar a aplicação adequada do princípio da segregação de funções, de for-ma que seja evitada a ocorrência de conflitos de interesse e fraudes;
e) Verificar o cumprimento do Código de Conduta e Integridade, bem como promover treinamentos periódicos aos empregados e dirigentes da empresa sobre o tema;
f) Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa;

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

h) Estabelecer planos de contingência para os principais processos de trabalho da organização;

i) Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal e ao Comitê de Auditoria;

j) Disseminar a importância da Conformidade e do Gerenciamento de Riscos, bem como a responsabilidade de cada área da empresa nestes aspectos;

k) Outras atividades correlatas definidas pelo Diretor ao qual se vincula.

9. Disposições finais

9.1. A presente política deve ser contextualizada aos padrões, normas e procedimentos aplicáveis, considerando as especificidades da EMDEC e seu modelo de negócio.

9.2. Os membros da Comissão de Conformidade e Gestão de Riscos, Administradores e Conselheiros deverão receber em sua posse e anualmente treinamento sobre controle interno, abrangendo o gerenciamento de riscos.

9.3. Os casos omissos serão decididos pela Diretoria Executiva da EMDEC.

9.4. A presente Política entrará em vigor na data de sua publicação e permanecerá vigente por prazo indeterminando.