tecnologia a serviço da cidade
procempa

POLÍTICA DE GESTÃO DE RISCOS, CONTROLES INTERNOS E CONFORMIDADE

1. Preâmbulo

Institui a Política de Gestão de Riscos, Controles Internos e Conformidade, com o objetivo de estabelecer o direcionamento estratégico da Gestão de Riscos, Controles Internos e Conformidade para a Procempa.

2. Objetivo

A presente Política de Gestão de Riscos, Controles Internos e Conformidade tem por finalidade estabelecer o direcionamento estratégico e as determinações para as atividades da Companhia de gestão de riscos, controles internos e conformidade, de forma a assegurar a integração aos processos organizacionais, reduzir a exposição a riscos, danos ao patrimônio e à imagem da Procempa; além de fortalecer os mecanismos de governança.
Esta Política tem por finalidade estabelecer as diretrizes adotadas pela Procempa na identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades da Companhia, incorporando a visão de riscos à tomada de decisões estratégicas, em consonância com as melhores práticas de mercado, nos termos da legislação aplicável em especial à Lei 13.303, de 30 de junho de 2016.

3. Âmbito da Aplicação

Esta Política aplica-se aos administradores, aos empregados do quadro regular, aos empregados em comissão, aos cedidos à Companhia e aos estagiários.

4. Definições e Conceitos

Para os efeitos desta Política, são adotados os seguintes conceitos e definições:

Alta Administração: pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível, ficando restrito esse conceito aos membros do Conselho de Administração e da Diretoria Executiva da Companhia;

Apetite a Risco: nível de risco que a organização está disposta a aceitar para atingir seus objetivos estratégicos e criar valor aos acionistas;

Área Proprietária do Risco: unidade organizacional que possui responsabilidade e autoridade pelo gerenciamento do risco;

Avaliação dos Riscos: processo onde são realizadas análises qualitativas ou quantitativas, ou ambas, para estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência, visando à definição dos atributos de probabilidade e impactos, utilizados na priorização dos riscos a serem tratados;

Conformidade: agir de acordo com uma regra; estar em concordância com as leis e os regulamentos externos e internos;

Controles Internos: são as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos da organização;

Fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

Gerenciamento de Riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos para aumentar a probabilidade de alcance dos objetivos da organização;

Gestão de Riscos: atividades coordenadas para dirigir e controlar uma organização a partir das volatilidades, complexidades e ambiguidades do negócio;

Governança: combinação de processos e estruturas implantadas pela alta administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos;

Governança no Setor Público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

Identificação de Riscos: processo de reconhecer e descrever os riscos aos quais a Companhia está exposta, envolvendo a identificação de eventos, fatores de risco e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

Nível de Risco: magnitude de um risco, expressa em termos da combinação de seu impacto e probabilidades de ocorrência;

Oportunidade: possibilidade de um evento ocorrer e influenciar positivamente a realização dos objetivos da organização;

Processo de Gestão de Riscos: processo de aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, resposta e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

Resiliência: capacidade de prevenir a ocorrência de ameaças potenciais ao negócio e, na impossibilidade, responder de forma eficaz a tais ameaças, recuperando rapidamente a normalidade após uma disrupção, minimizando perdas financeiras, danos reputacionais e quebra de obrigações contratuais, legais e regulamentares;

Risco: possibilidade de um evento ocorrer e afetar negativamente a realização dos objetivos da organização, podendo indicar uma oportunidade, quando o efeito de sua incidência for positivo, na forma do inciso XI deste artigo;

Risco Inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

Risco Residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

Riscos Financeiros / Orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

Riscos de Imagem/Reputação do Órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;

Riscos Legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;
Riscos Operacionais: eventos internos e externos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas de informação;

Tipologia de Riscos: forma de classificação dos riscos, de acordo com tipos específicos, para facilitar seu agrupamento e avaliação pela organização;

Tolerância aos Riscos: é a faixa de desvios em relação aos níveis de riscos determinados como aceitáveis pela Procempa, durante o desempenho de suas operações;

Tratamento de Riscos: processo para modificar o risco; e

Valor: é o resultado obtido mediante o alcance do bem-estar econômico, a alocação socialmente eficiente dos recursos geridos com sustentabilidade ambiental e responsabilidade social, e a eficácia na implementação de políticas públicas no setor em que atua, gerando maior retorno possível aos acionistas da Procempa;

5. Premissas

5.1 A Gestão de Riscos, Controles Internos e Conformidade são mecanismos de governança e de tomada de decisão, cuja finalidade é facilitar o alcance dos objetivos organizacionais utilizando as melhores práticas antifraude e anticorrupção, com o intuito de aprimorar e manter a transparência e a qualidade das informações divulgadas interna e externamente.

5.2 O comprometimento da alta direção é garantia da independência na execução dos mecanismos previstos nesta política.

5.3 A Gestão de Riscos, Controles internos e a Conformidade são parte integrante de todos os processos organizacionais e deve adotar uma linguagem padrão de gestão de riscos na Companhia possibilitando um melhor entendimento entre as partes e um processo livre de interferências.

5.4 Todos os gestores e empregados, em seus processos de atuação, são responsáveis pela Gestão de Riscos, Controles Internos e Conformidade, e serão orientados a elaborar e usar os instrumentos normativos e procedimentos para executar estas tarefas.

5.5 A organização da Gestão de Riscos, Controles Internos e Conformidades é estabelecida e mantida em ciclos de melhoria contínua, para permitir ajustes e a adaptação às mudanças organizacionais, com base em metodologias e padrões formalizados, reconhecidos pelo mercado e disseminados na Companhia.

5.6 A política integrada de gestão de riscos deve permear todas as práticas e processos organizacionais da Procempa, de forma a garantir a identificação de eventos de riscos inerentes a todas as áreas de negócio, compreendendo:

a) **Riscos operacionais:** vinculados a processos internos, pessoas, infraestrutura e sistemas de informação - além dos riscos de imagem/reputação, financeiros/orçamentários e legais; e
b) **Riscos estratégicos:** relacionados ao planejamento estratégico da organização.

6. Diretrizes

6.1 A metodologia de Gestão de Riscos e Controles Internos deve contemplar a sistemática e elementos utilizados para identificar, avaliar, priorizar, tratar, comunicar e monitorar os riscos a serem levados em consideração.

6.2 A Gestão de Riscos deve priorizar o tratamento dos processos que concentrem os riscos corporativos críticos. Este tratamento será conduzido pelo departamento responsável pela Gestão de Riscos – Departamento de Controladoria – P/CON, em conjunto com o gestor local do processo.

6.3 Para os processos que não concentrarem riscos corporativos

críticos, o tratamento dos riscos será realizado pelos responsáveis dos respectivos departamentos organizacionais por meio da auto aplicação da metodologia.

6.4 Indicadores de riscos e conformidade serão estabelecidos e monitorados respeitando o ciclo dos processos, servindo de base para tomada de decisão quanto aos limites de exposição aos riscos corporativos.

7. Metodologia de Gestão de Riscos

A Metodologia de Gestão de Riscos da Procempa busca estruturar as etapas para a operacionalização da Gestão de Riscos na Companhia, definindo um processo de gerenciamento de riscos, composto pelas seguintes etapas:

7.1 Entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;

7.2 Identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;

7.3 Análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;

7.4 Avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;

7.5 Priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

7.6 Definição de respostas aos riscos: etapa em que são definidas

as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas; e

7.7 Comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria.

8. Responsabilidades

A Procempa adota o posicionamento declarado pelo Instituto dos Auditores Internos do Brasil intitulado as Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles por considerar ser uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades afetas a cada um na organização.

Neste modelo, a primeira linha de defesa no gerenciamento de riscos, são os controles das Gerências operacionais. A segunda linha de defesa são as funções de controle de riscos e a supervisão de conformidades estabelecidas pelas gerências operacionais. Por fim, na terceira linha de defesa, estão as auditorias que farão as avaliações sobre a eficácia do gerenciamento de riscos e controle.

As áreas proprietárias de riscos devem atuar como primeira linha de defesa da Procempa, gerenciando de forma eficaz os riscos inerentes as suas atividades avaliando-os e tratando-os de modo a respaldar suas decisões.

A Gerência de Controladoria e o Comitê Estratégico de Gestão de Riscos, Controles e Segurança da Informação devem atuar na segunda linha de defesa da Companhia, ajudando a desenvolver os processos e os controles para gerencia os riscos da primeira linha de defesa, fornecer orientações e treinamento sobre

processos e gerenciamento de riscos e monitorar a implementação do gerenciamento de riscos por parte das áreas proprietárias do risco. Ainda na segunda linha de defesa compete a Gerência de Controladoria monitorar a adequação e a eficácia dos Controles Internos, a integridade dos processos de gerenciamento do risco e a conformidade com leis e regulamentos atuando na resolução das deficiências.

Por fim, na 3ª linha de defesa, está a Auditoria Interna que fará avaliações abrangentes, independentes e objetivas sobre a eficácia da governança, do gerenciamento de riscos e controles.

8.1 Compete ao Comitê Estratégico de Gestão de Riscos, Controles e Segurança da Informação:

a) Identificar riscos preventivamente e fazer sua necessária gestão, avaliando a probabilidade de ocorrência e adotando medidas para sua prevenção e minimização;
b) Implantar a gestão integrada dos riscos operacionais, financeiros e de segurança da informação da Procempa;
c) Implementar as estratégias e diretrizes aprovadas pelo Conselho de Administração;
d) Propor e implementar sistema de controles internos incluindo políticas e limites de alçada, alinhado ao nível de apetite e tolerância ao risco;
e) Supervisionar a institucionalização da gestão de riscos, de controles internos e conformidade.

8.2 Compete à Diretoria Executiva:

a) Designar o Comitê de Gestão de Riscos, responsável pela elaboração do Plano de Gestão de Riscos, que será composto por uma equipe multidisciplinar;
b) Propor ao Conselho de Administração o nível de apetite ao

risco;

c) Alocar recursos necessários ao processo e definir a infraestrutura apropriada às atividades de gerenciamento de riscos;
d) Validar os riscos considerando sua relevância e probabilidade de ocorrência.

8.3 O Conselho de Administração deliberará sobre as questões estratégicas concernentes ao processo de gestão de riscos, tais como:

a) Definir a estratégia da Companhia para atendimento de seus objetivos de negócio;
b) Definir o nível de apetite ao risco na condução dos negócios;
c) Aprovar os relatórios de controles internos, *compliance* e risco corporativo;
d) Aprovar a Política de Gestão de Riscos Corporativos, assim como suas revisões;
e) Aprovar o Plano de Gestão de Riscos da Companhia.

8.4 O Comitê de Auditoria Estatutário deverá:

a) Avaliar, monitorar os riscos aos qual a Companhia está exposta;
b) acompanhar a implementação das ações de resposta sugeridas pelo Comitê de Gestão de Riscos, pelo Conselho de Administração ou pela Diretoria;
c) revisar a estratégia de gerenciamento de riscos da Companhia, elaborando parecer ao Conselho de Administração.

8.5 A Gerência de Controladoria: deverá assessorar a Diretoria

Executiva na fixação de diretrizes e de controles sendo a unidade organizacional responsável pela gestão e operacionalização desta política na Procempa.

8.6 A Auditoria Interna: é responsável por aferir a efetividade do gerenciamento de riscos, a adequação dos controles internos e dos processos de governança.

8.7 Os gestores de processos organizacionais: são responsáveis por adotar medidas de gestão de riscos, de controles internos e conformidade, e verificar continuamente sua eficácia, para garantir o alcance dos objetivos Companhia.

8.8 Os Departamentos e Divisões: são responsáveis pela implementação desta política em seus segmentos de atuação, seguindo as orientações normativas emitidas sobre o tema.

9. Referências

Esta política encontra sua fundamentação na legislação vigente, bem como, no que couber, em padrões, técnicas e conceitos reconhecidamente adotados pelos órgãos de controle:

a) Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão;

b) Guia de Orientação para Gerenciamento de Riscos Corporativos do IBCG;

c) Lei 12.846/2013, de 01/08/2013, que dispõe sobre a responsabilidade administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública;

d) Lei 13.303, de 30/06/2016, que dispõe sobre o estatuto jurídico da Companhia pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;

e) ISO 31000:2009;

f) COSO (Committee of Sponsoring Organizations of the Treadway

Commission) I e II;

g) Norma de Política Corporativa de Gestão de Riscos, Controles Internos e Conformidade do Serpro;

h) Programa de Integridade da Prodabel;

i) Política de Gestão de Riscos da INFRAERO.

10. Disposições Finais

10.1 A P/CON emitirá orientações para adoção e implementação desta política, direcionadas aos Departamentos da Procempa.

10.2 As políticas e documentos organizacionais devem observar e serem ajustados, no que couber, às diretrizes desta política.

10.3 Cabe à P/CON dirimir dúvidas e coordenar ações para equacionar questões não previstas.

10.4 A não observância desta política e seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regime Disciplinar - Apuração de Responsabilidades e Aplicação de Penalidades e no Código de Ética e de Conduta da Procempa.

10.5 Esta política deve ser acompanhada pelo Conselho de Administração e pela Diretoria Executiva da Procempa quanto ao controle das diretrizes e procedimentos.

10.6 Os casos omissos serão decididos pela Diretoria Executiva.

tecnologia a serviço da cidade
procempa

Identificação	Política de gestão de riscos, controles internos e conformidade	
Assunto	Gestão de Riscos	
Área responsável	Controladoria – P/CON	
Público Alvo	Todos os órgãos da Procempa	
Anexos	N/A	
Início Vigência	13/12/2019	Atualização: N/A
Ato Normativo	ATA CA 408	