

**COMPANHIA ESPÍRITO SANTENSE DE SANEAMENTO – CESAN**



**POLÍTICA DE GERENCIAMENTO DE RISCOS**  
**INS.016.01.2022**

**CESAN**

<b>Revisão:</b> 01	<b>Proposta:</b> P-CRC	<b>Processo:</b> 2022.014509	<b>Aprovação:</b> Deliberação 4984/2022	<b>Páginas:</b> 09
-----------------------	---------------------------	---------------------------------	--	-----------------------

## DESCRIÇÃO DA ÚLTIMA ALTERAÇÃO

ITEM DA NORMA	DESCRIÇÃO DA ÚLTIMA ALTERAÇÃO
Item 3.9	Incluído – Partes Interessadas
Item 4, subitens 4.1 e 4.2	Alterado de Procedimentos para Diretrizes, alíneas de a) a f)
Item 5	Alterado de Documentos de Referência para Procedimentos, subitens 5.1 – Etapas do Gerenciamento de Riscos e 5.2 -Processo de Gestão de Riscos
Item 6	Alterado de Disposições Finais para Responsabilidades
Item 7	Documentos de Referência
Item 8	Disposições Finais

## SUMÁRIO

<b>1. OBJETIVO</b> .....	<b>3</b>
<b>2. COMPETÊNCIAS</b> .....	<b>3</b>
<b>3. DEFINIÇÕES</b> .....	<b>3</b>
3.1 ADMINISTRADORES.....	3
3.2 CONTROLES.....	3
3.3 RISCOS.....	3
3.4 MATRIZ DE RISCOS (MATRIZ DE PROBABILIDADE E IMPACTO).....	4
3.5 APETITE AO RISCO.....	4
3.6 TOLERÂNCIA AO RISCO.....	4
3.7 CAPACIDADE DE RISCOS.....	4
3.8 ÁREA PROPRIETÁRIA DO RISCO.....	4
3.9 PARTES INTERESSADAS.....	4
<b>4. DIRETRIZES</b> .....	<b>5</b>
<b>5. PROCEDIMENTOS</b> .....	<b>5</b>
5.1 ETAPAS DO GERENCIAMENTO DE RISCOS.....	5
5.2 PROCESSO DE GESTÃO DE RISCOS.....	7
<b>6. RESPONSABILIDADES</b> .....	<b>8</b>
<b>7. DOCUMENTOS DE REFERÊNCIA</b> .....	<b>9</b>
<b>8. DISPOSIÇÕES FINAIS</b> .....	<b>9</b>

## **1. OBJETIVO**

Estabelecer as diretrizes a serem observadas no processo de gestão de riscos da CESAN.

## **2. COMPETÊNCIAS**

A atualização desta Política é de competência da Área de Riscos e Conformidade.

## **3. DEFINIÇÕES**

### **3.1 ADMINISTRADORES**

São os membros do Conselho de Administração e da Diretoria da CESAN.

### **3.2 CONTROLES**

Políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos da CESAN sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.

### **3.3 RISCOS**

Possibilidade de ocorrência de eventos que afetem a capacidade da CESAN de atingir seus objetivos. São inerentes a qualquer atividade e podem afetar os ativos, resultados, imagem ou continuidade dos negócios.

### 3.4 MATRIZ DE RISCOS (MATRIZ DE PROBABILIDADE E IMPACTO)

Ferramenta de gerenciamento de riscos que permite avaliar a priorização dos riscos.

### 3.5 APETITE AO RISCO

Grau de exposição a riscos que a Companhia está disposta a aceitar para atingir seus objetivos estratégicos, em busca de valor organizacional. O apetite ao risco pode ser alterado periodicamente, de acordo com as mudanças nos objetivos estratégicos e disponibilidade de recursos.

### 3.6 TOLERÂNCIA AO RISCO

Grau de variação do apetite ao risco que a Companhia está disposta a tolerar.

### 3.7 CAPACIDADE DE RISCOS

Risco máximo que a Companhia pode assumir a partir de sua capacidade financeira.

### 3.8 ÁREA PROPRIETÁRIA DO RISCO

Área responsável por definir as ações de mitigação dos riscos.

### 3.9 PARTES INTERESSADAS

Sociedade, acionistas, governo, órgãos regulamentadores, órgãos de controle, empregados, fornecedores, empresas contratadas, prefeituras municipais, entre outros.

## **4. DIRETRIZES**

- a) A CESAN considera sua missão, visão, cultura, estratégias anteriores e capacidade de riscos para definir seu apetite ao risco.
- b) A CESAN adota as melhores práticas de governança corporativa, pautada em uma visão sistemática que oportuniza a realização dos objetivos estratégicos, prezando sempre pela transparência.
- c) A CESAN possui o planejamento estratégico como ponto focal no seu processo de gerenciamento de riscos, nesse sentido, concilia as suas estratégias com o apetite ao risco e outros fatores externos, como órgãos reguladores e fiscalizadores.
- d) A gestão de riscos estará presente em todos os processos organizacionais, no entanto, priorizará aqueles que possuem um potencial de impacto mais severo.
- e) A gestão de riscos é avaliada periodicamente pelos Administradores e pela área de Riscos e Conformidade, e o resultado da avaliação é comunicado às principais partes interessadas.
- f) A classificação dos riscos identificados ocorre de acordo com a sua natureza, podendo ser riscos corporativos, estratégicos, financeiros, de integridade, de mercado, de conformidade (legais ou regulatórios) e operacionais. Assim, no momento de avaliar a classificação do risco envolvido, será feita análise de impacto (de acordo com a ponderação dos impactos, ou seja, se o risco tratado impacta em erros nas decisões estratégicas, sanções legais/regulatórias, perdas financeiras, operacionais e/ou de imagem, erros das demonstrações financeiras etc.) e análise de probabilidade, sendo esta relacionada ao ambiente de controles internos existente na Companhia e sua eficácia.

## **5. PROCEDIMENTOS**

### **5.1 ETAPAS DO GERENCIAMENTO DE RISCOS**

- a) **Identificação:** definir o conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da CESAN, devendo ser realizada em todos os níveis da Companhia, considerando-se os eventos passados (tendências) e possibilidades futuras. Para tanto podem ser utilizados os métodos: inventários de eventos, questionários e pesquisas, principais indicadores de eventos e gatilhos de escalação, brainstorming, análise SWOT (forças, fraquezas, oportunidades e ameaças), análise de cenários etc.
- b) **Análise:** verificar a gravidade do problema, a urgência na sua resolução e tendência de agravamento do problema, promovendo avaliação de riscos de maneira formal ou informal. Deve considerar avaliação da materialidade, probabilidade de um evento e consideração dos meios de gerenciar o risco. O resultado da avaliação é usado para priorizar riscos e produzir informações para a tomada de decisões, sendo que os métodos de avaliação de riscos podem ser qualitativos (listas de todos os riscos, ranking e mapas de riscos) e/ou quantitativos (modelos de probabilidade).
- c) **Tratamento:** definir qual o tratamento a ser adotado, considerando que as estratégias para resposta ao risco incluem evitar, reter, reduzir (mitigar) e compartilhar.
- d) **Identificação da área proprietária do risco:** a área responsável por definir as ações de mitigação do risco será definida pelas diretorias das áreas, em conjunto da área responsável pelo processo, com o suporte da área de Riscos e Conformidade.
- e) **Monitoramento:** a área proprietária do risco deverá avaliar, no mínimo mensalmente, através de indicadores, se os riscos estão com tendência de melhoria, adotando medidas corretivas se necessário. A área de Riscos e Conformidade fará a avaliação dos planos atuais de resposta aos riscos, bem como se há identificação de novos riscos.
- f) **Verificação de cumprimento de obrigações e de gestão de riscos:** a unidade de Riscos e Conformidade deverá avaliar a adequação e eficácia das atividades de controle e obter informações que proporcionem melhorias no processo de gerenciamento de riscos.

- g) Comunicação: a área de Riscos e Conformidade deverá comunicar os resultados aos Administradores, ao final do processo de identificação, avaliação e análise dos riscos, por meio de envio do arquivo consolidado da Matriz de Riscos e Controles, contendo a classificação dos riscos como baixo, médio e alto. Os riscos serão tratados pelas áreas proprietárias dos riscos, com o apoio da área de Riscos e Conformidade e da Diretoria.
- h) Contexto: estabelecer identificação de contextos significantes dentro dos quais os riscos devem ser gerenciados, como por exemplo, leis e regulamentos, tecnologia, organizações, processos de negócios etc.

## 5.2 PROCESSO DE GESTÃO DE RISCOS

- a) Em todas as unidades da CESAN devem ser estabelecidos controles com o objetivo de prevenir ou detectar e corrigir eventos indesejáveis, de forma a garantir o cumprimento das diretrizes determinadas pelos Administradores da CESAN;
- b) O processo de gestão de riscos da CESAN está baseado no planejamento estratégico e deve considerar os aspectos identificados na Matriz de Riscos e Controles, bem como aqueles inerentes à missão, visão, valores e objetivos estratégicos da Companhia.
- c) Os riscos são desdobrados nos planos de trabalho das Áreas para tratamento e monitoramento;
- d) Os Gestores devem monitorar e tratar os riscos das unidades sob sua responsabilidade;
- e) Os Diretores devem apresentar o plano de negócios para o exercício anual seguinte, até a última reunião ordinária do Conselho de Administração do ano anterior, e a estratégia de longo prazo atualizada com análise de riscos e oportunidades para, no mínimo, os próximos 5 (cinco) anos.
- f) As unidades responsáveis pelos riscos devem apresentar no final do exercício um resumo das ações realizadas para sua mitigação, que servirá de base para a avaliação anual do Plano de Negócios.
- g) O Conselho de Administração promoverá, anualmente, análise de atendimento das metas e resultados na execução do plano de negócios e



- da estratégia de longo prazo e dos riscos, devendo publicar suas conclusões em relatório de prestação de contas, disponível no site da CESAN a todas as partes interessadas.
- h) Os Administradores devem promover a gestão de riscos em todos os níveis hierárquicos e áreas de atuação da CESAN;
  - i) A Matriz de Riscos da CESAN deve ser revisada periodicamente, considerando o rumo dos acontecimentos relacionados aos objetivos estratégicos;
  - j) O monitoramento contínuo dos riscos é realizado pelos Administradores e pelo Comitê de Auditoria, através da análise periódica de indicadores.
  - k) Deve ser realizado treinamento periódico, no mínimo anual, sobre a política de gestão de riscos aos Administradores.
  - l) O Comitê de Auditoria Estatutário deve se comunicar com o Conselho de Administração a respeito do apetite ao risco, tolerância ao risco e o gerenciamento de riscos, de modo que após análise do planejamento estratégico possa determinar se os objetivos estratégicos estão alinhados com a missão, visão e apetite ao risco.
  - m) A Área de Riscos e Conformidade deve promover avaliação periódica do apetite ao risco junto aos Administradores.

## **6. RESPONSABILIDADES**

- a) Conselho de Administração: implementar e supervisionar o sistema de gestão de riscos.
- b) Diretoria: colocar em prática e assegurar a efetividade do sistema de gestão de riscos.
- c) Comitê de Auditoria Estatutário: avaliar e monitorar as exposições de risco da CESAN, podendo inclusive requerer informações a respeito de utilização de ativos e despesas ocorridas, bem como fornecer suporte para Área de Riscos e Conformidade em assuntos específicos, como potenciais áreas de risco às demonstrações financeiras, supervisionando o trabalho realizado a partir de uma compreensão sobre o negócio e os riscos significativos a que a Companhia está exposta.

- d) Auditoria Interna: aferir a efetividade do gerenciamento de riscos.
- e) Área de Riscos e Conformidade: promover e orientar a aplicação de normas, diretrizes e procedimentos de gestão de riscos.
- f) Gestores: aplicar os componentes do sistema de gestão de riscos e das atividades de controles.
- g) Empregados: atuar junto aos gestores na implementação de ações necessárias ao tratamento dos riscos e contribuir para o aperfeiçoamento do modelo de Gestão de Riscos da CESAN.

## **7. DOCUMENTOS DE REFERÊNCIA**

**ENTERPRISE RISK MANAGEMENT. INTEGRATING WITH STRATEGY AND PERFORMANCE 2017 - COSO**

**ESTATUTO SOCIAL – CESAN**

**EVOLUÇÃO EM GOVERNANÇA E ESTRATÉGIA 2017 – IBGC**

**GUIA DE ORIENTAÇÃO PARA GERENCIAMENTO DE RISCOS CORPORATIVOS 2007 - IBGC**

**MG-01-003 - IDENTIFICAÇÃO, CLASSIFICAÇÃO E TRATAMENTO DOS RISCOS EMPRESARIAIS - MANUAL DE GESTÃO – CESAN**

**LEI FEDERAL Nº 12.846/2013** - 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.

**LEI FEDERAL Nº 13.303/2016** - 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.

**THE INSTITUTE OF INTERNAL AUDITORS**

## **8. DISPOSIÇÕES FINAIS**

Os casos omissos nesta Política são resolvidos a critério do Conselho de Administração.