DELIBERAÇÃO Nº 5081/2023

APROVAR A POLÍTICA DE GERENCIAMENTO DE RISCOS

O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA ESPÍRITO SANTENSE DE SANEAMENTO - CESAN, usando de atribuições que lhe são conferidas pelo Estatuto,
RESOLVE:

Artigo 1º - Revogar a Política INS.016.01.2022 – Gerenciamento de Riscos.

Artigo 2º - Aprovar a Política INS.016.02.2023 – Gerenciamento de Riscos.

Artigo 3º - Esta Deliberação entra em vigor nesta data, revogadas as disposições em contrário, em especial as contidas na Deliberação nº 4984/2022.

Vitória, 28 de novembro de 2023.

ERICO SANGIORGIO:08092448701 Assinado digitalmente por ERICO SANGIORGIO:08092448701 Data: 2023.12.04 18:17:07 -0300

Érico Sangiorgio
PRESIDENTE DO C.A.

MUNIR ABUD DE OLIVEIRA:11375975773 Assinado de forma digital por MUNIR ABUD DE OLIVEIRA:11375975773 Dados: 2023.11.29 18:57:12 -03'00'

Munir Abud de Oliveira
CONSELHEIRO

PEDRO MENEGUETTI:41835484620 Assinado de forma digital por PEDRO MENEGUETTI:41835484620 Dados: 2023.12.04 17:10:00 -03'00'

Pedro Meneguetti
CONSELHEIRO

JOSE ALVES PAIVA:04980034772 Assinado de forma digital por JOSE ALVES PAIVA:04980034772 Dados: 2023.12.01 08:48:02 -03'00'

José Alves Paiva
CONSELHEIRO

PEDRO CACADOR NETO:09464368780 Assinado de forma digital por PEDRO CACADOR NETO:09464368780 Dados: 2023.12.01 16:46:59 -03'00'

Pedro Caçador Neto
CONSELHEIRO

JOSE MARCOS TRAVAGLIA:56063601791 Assinado de forma digital por JOSE MARCOS TRAVAGLIA:56063601791 Dados: 2023.11.29 17:08:53 -03'00'

José Marcos Travaglia
CONSELHEIRO

FABIANO CUZINI SCARPINI Assinado de forma digital por FABIANO CUZINI SCARPINI Dados: 2023.11.30 22:24:14 -03'00'

Fabiano Cuzini Scarpini
CONSELHEIRO

1012ª Reunião do C.A.
Processo nº 2023.014225

COMPANHIA ESPÍRITO SANTENSE DE SANEAMENTO – CESAN

POLÍTICA DE GERENCIAMENTO DE RISCOS

INS.016.02.2023

Revisão:	Proposta:	Processo:	Aprovação:	Páginas:
02	P-CRC	2023.014225	Deliberação 5081/2023	10

DESCRIÇÃO DA ÚLTIMA ALTERAÇÃO

ITEM	DESCRIÇÃO DA ÚLTIMA ALTERAÇÃO
Toda a política	Revisado todo o conteúdo.

SUMÁRIO

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 Conselheiros de Administração e Diretores 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. Os riscos podem ser relacionados a eventos estratégicos, operacionais, financeiros, regulatórios ou de projetos, de acordo com sua ocorrência nas esferas de governança e gestão dos processos da Companhia.

3.4 MATRIZ DE RISCOS

Ferramenta de gerenciamento de riscos que permite avaliar a priorização de tratamento dos riscos a partir do nível de exposição de cada um dos riscos nela contidos. Na CESAN, de acordo coma alçada de mapeamento dos riscos, as seguintes matrizes podem ser categorizadas: Matriz Estratégica (relacionada aos eventos estratégicos), Matrizes Táticas (relacionadas a eventos por função ou unidade de negócio), Matrizes Operacionais (relacionadas a eventos por processos de negócio) e Matriz de Projetos (relacionadas a eventos por projetos corporativos).

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

Categorização do nível de exposição dos riscos da CESAN: INTOLERÁVEL, TOLERÁVEL, ACEITÁVEL. Trata-se da base metodológica para o estabelecimento do apetite ao risco e do eventual tratamento do risco (estabelecimento de planos de ação para mitigação de riscos).

3.7 GESTOR DO RISCO

Gestor da CESAN responsável pelo reporte à estrutura de governança e gestão da Companhia sobre a situação do processo de gestão dos riscos sob sua responsabilidade: (1) identificação dos riscos e seus fatores, (2) análise e estabelecimento de premissas de impacto/probabilidade (nível de exposição do risco), (3) estabelecimento de planos de ação para mitigação dos riscos e (4) *follow-up* dos planos de ação: diligenciamento tempestivo da implementação

desses planos (efetividade na gestão dos riscos da CESAN). Cabe ao gestor do risco a nomeação dos AGENTES DE RISCOS para suporte técnico na consecução das atribuições de gestão do risco (delegação de autoridade para identificação, análise, avaliação, tratamento e follow-up do risco), com o devido suporte metodológico da Área de Riscos e Conformidade.

3.8 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 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, táticos, operacionais e de projetos prezando sempre pela transparência.
c) A CESAN possui o planejamento estratégico como ponto de referência principal 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 nível de exposição intolerável, alinhado ao seu apetite ao risco.
e) A gestão de riscos é avaliada periodicamente pelos Administradores, pelos seus respectivos gestores nominados, com o suporte metodológico da 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, estratégicos, financeiros, de integridade, de

mercado, de conformidade (legais ou regulatórios), operacionais e de projetos. Assim, no momento de avaliar o nível de exposição do risco envolvido, tendo como referência seus fatores de risco, 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.

g) A Matriz de Riscos é a ferramenta utilizada para apresentação do nível de exposição dos riscos. Cada matriz de risco (estratégica, tática, operacional ou de projetos) possui o seu respectivo critério para estabelecimento das métricas de impacto (quantitativo/financeiro ou qualitativo) e probabilidade.
h) O tratamento dos riscos deve ser feito após análise do nível de exposição de cada risco da matriz: eliminação, redução, aceitação ou transferência do risco. A partir do apetite e tolerância a riscos da CESAN, para os casos que ensejam tratamento, devem ser estabelecidos planos de ação que serão periodicamente monitorados em sua efetividade pelos Administradores: implantado, em andamento (no prazo), atrasado, revisado (com a prévia validação metodológica da área de Riscos e Conformidade) ou cancelado (quando houver mudança significativa do contexto do risco). O monitoramento dos riscos da CESAN deve ser item permanente da agenda dos instrumentos de governança e gestão da Companhia.

5. PROCEDIMENTOS

5.1 ETAPAS DO PROCESSO DE GESTÃO DE RISCOS

a) Identificação: definir o conjunto de eventos, externos ou internos e seus respectivos fatores, que podem impactar os objetivos dos processos de governança e gestão 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) Identificação do Gestor do Risco: nominação do Gestor da Companhia responsável pelo reporte à estrutura de governança e gestão sobre a situação dos riscos sob sua responsabilidade (identificação, análise, avaliação, tratamento e monitoramento preventivo). O Gestor do Risco é responsável pela indicação e nomeação dos agentes de riscos para suporte técnico na delegação de atribuições no processo de gestão do risco.

c) Análise: verificar a gravidade do evento, a urgência na sua resolução e tendência de agravamento do evento, promovendo avaliação de riscos de maneira quantitativa e/ou qualitativa. 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 através do nível de exposição apresentado na matriz de riscos.

d) Tratamento: definir, em função do apetite e tolerância a riscos, qual o tratamento a ser adotado, considerando que as estratégias para resposta ao risco incluem eliminação, redução, aceitação ou transferência do risco.

e) Monitoramento: o gestor 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 de resposta aos riscos, bem como se há identificação de novos riscos.

f) Verificação de cumprimento de obrigações e de gestão de riscos: a Área 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

extremo, alto, médio, baixo ou muito baixo. Os riscos serão tratados pelos gestores 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 ORIENTAÇÕES GERAIS DO 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 metas e objetivos determinados pelos Administradores da CESAN;
b) O processo de gestão de riscos da CESAN está baseado nos objetivos encontrados na sua missão, visão, valores, planejamento estratégico e processos de negócio.
c) Os gestores dos riscos devem apresentar nas reuniões de acompanhamento da estratégia um resumo das ações realizadas para sua mitigação, que servirá de base para a avaliação anual do Plano de Negócios.
d) 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.
e) Os Administradores devem promover a gestão de riscos em todos os níveis hierárquicos, processos e áreas de atuação da CESAN;
f) A Matriz de Riscos da CESAN deve ser revisada periodicamente, considerando o rumo dos acontecimentos relacionados aos objetivos estratégicos e/ou dos processos de negócio;
g) O monitoramento contínuo dos riscos é realizado pelos Administradores, através da análise periódica de indicadores.

h) Deve ser realizado treinamento periódico, no mínimo anual, sobre a política de gestão de riscos aos Administradores.
i) 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 modelo de gestão de riscos.
c) Auditoria Interna: aferir a efetividade na aplicação do modelo de gerenciamento de riscos.
d) Área de Riscos e Conformidade: promover e orientar a aplicação de normas, diretrizes e procedimentos de gestão de riscos.
e) Gestores: aplicar os componentes do modelo de gestão de riscos e das atividades de controles.
f) 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 CORPORTATIVOS 2007 - IBGC

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.