

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DA CAGECE

REVISÃO Nº 06

1. APRESENTAÇÃO

1.1 A Política de Gestão de Riscos Corporativos da Cagece tem por finalidade fornecer diretrizes para identificação e gerenciamento dos riscos que possam vir a impactar em sua estratégia.

1.2 Esta Política é incentivada e orientada pela Administração e aplica-se a toda Companhia.

1.3 O processo de gestão de riscos corporativos da Cagece tem como base o modelo internacional COSO ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management, as normas ABNT NBR ISO 31000, ABNT NBR 31.073:2022 e o Modelo das Três Linhas do Instituto de Auditores Internos do Brasil – IIA Brasil.

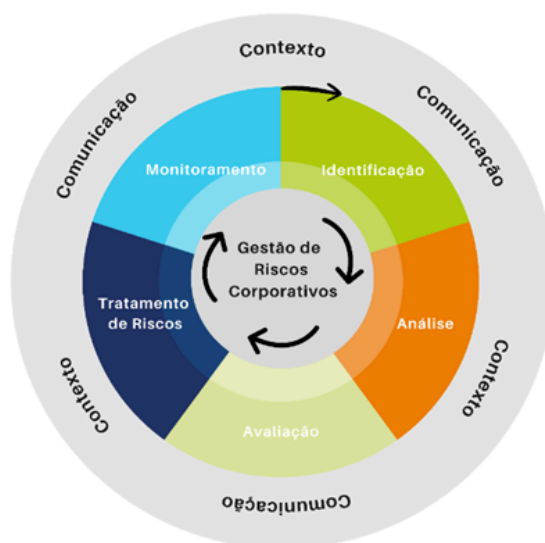


Figura 1- Modelo de Gestão de Riscos da Cagece.

2. FUNDAMENTAÇÃO LEGAL

2.1 Lei Federal n.º 13.303/2016 de 30/06/2016 e alterações posteriores;

2.2 COSO® ERM e alterações posteriores;

2.3 COSO® ICIF e alterações posteriores;

2.4 ABNT NBR ISO 31000:2018 e alterações posteriores;

2.5 ABNT NBR ISO 31.073:2022 e alterações posteriores;

2.6 ABNT NBR ISO/IEC 31010:2012 e alterações posteriores;

2.7 Decreto Estadual Nº33.805, de 09/11/2020 e alterações posteriores

3. DEFINIÇÕES E CONCEITOS

3.1 ABNT – Associação Brasileira de Normas Técnicas;

3.2 AGR – Análise Geral de Risco AGR –A AGR tem como objetivo identificar e classificar os principais riscos vinculados às atividades, áreas e estrutura da companhia, verificando as origens e fatores que evidenciam o nível de exposição ao risco da Cagece;

3.3 APETITE AO RISCO – A quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão) [COSO® ERM]. O apetite ao risco reflete a filosofia de gerenciamento de riscos da companhia. Quantidade e tipos de riscos que uma organização está disposta a buscar ou reter. [ABNT NBR ISO 31.073:2022 , item 3.3.27];

3.4 ANÁLISE DE RISCO - Etapa do modelo de gestão de riscos corporativos que consiste no processo de compreender a natureza do risco. Fornece base para a avaliação de riscos (risk evaluation) e para as decisões sobre o tratamento de riscos (ABNT NBR ISO 31073:2022, item 3.3.15)

3.5 AVALIAÇÃO DE RISCO - Etapa do modelo de gestão de riscos que consiste no processo de comparar os resultados das análises de riscos com os critérios de risco para determinar se o risco é aceitável ou tolerável [ABNT NBR ISO 31.073:2022 item 3.3.25]

3.6 COSO® ERM – *Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management*; denominação dada ao *framework* desenvolvido pelo Comitê Patrocinador da Comitê das Organizações Patrocinadoras da Comissão *Treadway* voltado para a gestão de riscos integrada a estratégia.

3.7 COSO® ICIF - *Committee of Sponsoring Organizations of the Treadway Commission - Internal Control – Integrated Framework*: denominação dada ao *framework* desenvolvido pelo Comitê Patrocinador da Comitê das Organizações Patrocinadoras da Comissão *Treadway* voltado para o controle interno.

3.8 COMUNICAÇÃO – Etapa do modelo de gestão de riscos corporativos que ocorre no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos. Refere-se ao reporte de riscos que é a forma de comunicação destinada a informar partes interessadas específicas, internas ou externas, fornecendo informações relativas ao estado atual do risco e sua gestão. ((ABNT NBR ISO 31.000:2018 item 6.2 e ABNT NBR ISO 31.073:2022 item 3.3.42). A comunicação é bidirecional; não é apenas informar, mas também ouvir;

3.9 CONTEXTO – É o ambiente, interno ou externo, no qual a organização está inserida e busca atingir seus objetivos. O contexto interno pode incluir estrutura organizacional, funções, responsabilidades, políticas, estratégias, percepções, valores, cultura organizacional, etc.; O contexto externo pode incluir ambiente cultural, social, político, legal, regulatório, financeiro, econômico, tecnológico, tendências, relações com partes interessadas, etc.; devendo ser considerado em todas as etapas do modelo [ABNT NBR ISO 31.073:2022 itens 3.3.4 e 3.3.5];

3.10 CONTROLE INTERNO – Processo efetuado pelo conselho, administração ou qualquer outro funcionário de uma empresa, desenhado para fornecer garantia razoável em relação à realização dos objetivos [COSO® ICIFI] nas seguintes categorias: Eficácia e eficiência das operações, Confiabilidade dos relatórios financeiros, Conformidade com leis e regulamente aplicáveis.

3.11 DICIONÁRIO DE RISCOS - Compilação de palavras, locuções, termos e expressões, classificadas por temas e categorias específicas, organizadas numa ordem convencionada, usadas para descrever os riscos aos quais a Cagece está exposta. O dicionário de riscos da Cagece contempla ainda termos usados para indicar causas, consequências e controles.

3.12 EVENTO DE RISCO: O evento é a ocorrência ou mudança em um conjunto específico de circunstâncias que pode ser fonte de risco quando trata-se de um elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco [ABNT 31000];

3.13 GESTÃO DE RISCOS – Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. [ABNT NBR ISO 31.073:2022 , item 3.2.1]

3.14 GESTÃO DE RISCOS CORPORATIVOS – Processo de avaliação que permite que uma organização considere até que ponto os fatores de riscos em potencial podem impactar na realização dos objetivos;

3.15 GOVERNANÇA CORPORATIVA – Conforme definido pelo Instituto Brasileiro de Governança Corporativa (IBGC), governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle;

3.16 GRAU DE EXPOSIÇÃO – Grau em que uma organização ou parte interessada está sujeita a um evento. [ABNT NBR ISO 31.073:2022 , item 3.3.17];

3.17 GRC – Ge rência de Governança, Riscos e Conformidade;

3.18 GRC-RCP – Coordenadoria de Gestão de Riscos, Controles Internos e Processos;

3.19 IBGC – Instituto Brasileiro de Governança Corporativa;

3.20 ISO – *International Organization for Standardization* ;

3.21 IDENTIFICAÇÃO DE RISCOS – – Etapa do modelo de gestão de riscos corporativos que corresponde ao processo de busca, reconhecimento e descrição de riscos. A identificação de riscos envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais. Pode envolver dados históricos, análises teóricas, opiniões de pessoas especialistas e as necessidades das partes Interessadas; [ABNT NBR ISO 31.073:2022 , item 3.3.9]

3.22 IMPACTO – Resultado ou efeito de um evento de risco. Poderá haver uma série de impactos possíveis associados a um único evento. O impacto pode ser positivo ou negativo em relação ao alcance dos objetivos;

3.23 KRI – *Key Risk Indicator* (Indicador Chave de Risco) – são métricas e dados que permitem a visualização, acompanhamento e gestão de incertezas, ameaças ou prejuízos em potencial para um negócio. São componentes do processo de monitoramento de riscos que são utilizados para fornecer indicadores antecipados de condições de risco em potencial e podem funcionar como indicadores de controle ao sinalizar que um controle não está funcionando corretamente;

3.24 MAPA DE RISCO – Representação gráfica referente ao processo de avaliação de riscos no ambiente corporativo apresentado no layout de Mapa 5 x 5, através de posicionamento do nível de risco em quadrante com cor correspondente representado no plano cartesiano por partes ordenadas (probabilidade e impacto); Também recebe a denominação de matriz de riscos;

3.25 MONITORAMENTO – Etapa do modelo de gestão de riscos corporativos que corresponde ao processo de verificação, supervisão, observação crítica ou identificação de situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado após implementação do Plano de Ação [ABNT NBR ISO 31.073:2022 item 3.3.40].

3.26 PROBABILIDADE – Chance de um evento acontecer. Na terminologia de gestão de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo).Fonte: ISO 31000: 2018;

3.27 PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS – Compreende as atividades de identificação, análise, avaliação e resposta aos riscos, comunicação e monitoramento dos riscos internos capazes de afetar o alcance dos objetivos da Cagece;

3.28 PROPRIETÁRIO DO RISCO – Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar riscos. [NBR ISO 31073:2022, item 3.3.14];

3.29 RISCO – Conforme definido no COSO® ERM, risco é a possibilidade de ocorrência de um evento, oriunda de fontes internas ou externas, capaz de afetar adversamente o atendimento dos objetivos da companhia. É o efeito da incerteza nos objetivos [NBR ISO 31073:2022, item 3.1.1];

3.30 RISCO DE NEGÓCIO – Exposição aos impactos, resultantes de decisões ou eventos, internos ou externos, de natureza estratégica, operacional, financeira, legal e outras decorrentes da maneira pela qual a organização busca atingir os seus objetivos;

3.31 TOLERÂNCIA AO RISCO – A variação aceitável relativa à realização de um objetivo [COSO® ERM]. Disposição da organização ou parte interessada em suportar o risco residual, a fim de atingir os seus objetivos. A tolerância ao risco pode ser influenciada por requisitos legais ou regulatórios. [NBR ISO 31073:2022, item 3.3.28].

3.32 TRATAMENTO DE RISCOS - Etapa do modelo de gestão de riscos corporativos que corresponde ao processo para selecionar e implementar opções para abordar riscos. O tratamento de riscos pode envolver: evitar o risco, assumir o risco para buscar uma oportunidade, remover a fonte do risco, alterar a probabilidade ou as consequências, compartilhar o risco ou reter o risco por decisão informada [ABNT NBR ISO 31.073:2022 , item 3.3.32]

4. OBJETIVOS

4.1 Estabelecer princípios, diretrizes e competências a serem observadas no processo de gestão de riscos corporativos da Cagece, de forma a assegurar a identificação, análise, avaliação, priorização, tratamento, monitoramento e comunicação dos riscos do negócio com o propósito de contribuir para a sustentabilidade da Companhia e apoiar os processos decisórios;

4.2 Promover e disseminar uma cultura de conformidade e de atuação proativa a fim de ampliar a capacidade da rede de governança;

4.3 Aperfeiçoar procedimentos e práticas de gestão de riscos corporativos em todos os níveis hierárquicos da organização com intuito de mitigar os riscos e apoiar o alcance dos objetivos estratégicos;

4.4 Promover uma linguagem comum e difundir o conhecimento sobre gestão de riscos.

5. DIRETRIZES E PRINCÍPIOS

5.1 A estratégia empresarial e os processos de negócio devem considerar a gestão de seus riscos;

5.2 A prática de Gestão de Riscos na Cagece deve estar alinhada com a Missão, Visão, Valores e Objetivos Estratégicos da Companhia;

5.3 A Gestão de Riscos deve ser realizada de forma sistemática nos processos e macroprocessos organizacionais, constantes na cadeia de valor, conforme padrão estabelecido pela Cagece, seguindo metodologia adotada e definida no Manual de Gestão de Riscos da Cagece;

5.4 Os riscos dos processos e macroprocessos devem ser identificados, analisados, avaliados, tratados, comunicados e monitorados com o objetivo de mitigar o impacto às estratégias da Companhia e o cumprimento de seus objetivos;

5.5 Todos os envolvidos no processo de Gestão de Riscos Corporativos da Cagece devem estar capacitados na metodologia aplicada na Cagece;

5.6 Os riscos identificados devem ser classificados de acordo com o dicionário de riscos da cagece

5.7 Deve ser realizada de forma periódica, a cada dois anos, após a conclusão da AGR, uma avaliação da maturidade do processo de gestão de riscos;

5.8 O nível de criticidade dos riscos deve ser avaliado e definido de acordo com o nível do risco residual;

5.9 A Gerência de Governança, Riscos e Conformidade deve promover ampla discussão com as áreas para o desenvolvimento do processo de gestão de riscos;

5.10 A elaboração dos planos de resposta ao risco deve ser feita com base nos resultados das avaliações do nível de criticidade de cada risco;

5.11 A gestão de riscos corporativos é um processo dinâmico e interativo, com natureza proativa, para antecipar e responder a eventos, externos e internos, que possam alterar o contexto ou posicionamento estratégico da companhia. Por isso deve ocorrer por ciclos de avaliações e revisões frequentes ou em resposta a um fato específico, favorecendo a melhoria contínua e o fortalecimento das diretrizes estratégicas empresariais.

6. CARACTERÍSTICAS

6.1 A gestão de riscos corporativos deve ocorrer com o uso de linguagem comum e padrões estabelecidos na política e manual de Gestão de Riscos da Cagece;

6.2 As competências do Conselho de Administração, Conselho Fiscal, Comitê de Auditoria Estatutária, Diretoria Executiva, Comitê de Gestão de Riscos Corporativos, gestores de negócio, Gerência de Governança, Riscos e Conformidade por meio de suas Coordenações, e Auditoria Interna estão definidas no Anexo I desta política;

6.3 Os limites de tolerância são definidos com base na variação aceitável do apetite ao risco, definidos com base na filosofia de riscos adotada pela Diretoria Executiva e Conselho de Administração. Tais limites são definidos pela Diretoria Executiva e Conselho de Administração e balizam a classificação da avaliação dos riscos e processos nas dimensões "probabilidade" e "impacto".

Probabilidade

FATORES DE ANÁLISE					GRAU DE EXPOSIÇÃO	PONTUAÇÃO
Pessoas	Tecnologia da informação	Infraestrutura	Processo	Ambiente externo		
Nível <u>muito alto</u> de influência para a materialização do risco					Diário	5 - Muito Alto
Nível <u>alto</u> de influência para a materialização do risco					Quinzenal	4 - Alto
Nível <u>moderado</u> de influência para a materialização do risco					Mensal	3 - Médio
Nível <u>leve</u> de influência para a materialização do risco					Anual	2 - Baixo
Nível <u>muito leve</u> de influência para a materialização do risco					Eventual	1 - Muito Baixo

Tabela 1: Critérios para a avaliação da Probabilidade

Impacto

FATORES DE ANÁLISE	Imagem	Financeiro	Legal	Operacional	PONTUAÇÃO
PESO	2	4	4	5	
Orientações para análise	De carácter nacional	Acima de 2% da receita líquida	Perturbações muito graves	Impacta outros processos muito fortemente	5 - Catastrófico
	De carácter estadual	Entre 1% e 2% da receita líquida	Perturbações graves	Impacta outros processos de forma direta	4 - Severo
	De carácter regional	Entre 0,5% e 1% da receita líquida	Perturbações limitadas	Impacta somente o próprio processo consideravelmente	3 - Moderado
	De carácter interno – Dentro da organização	Entre 0,1% e 0,5% da receita líquida	Perturbações leves	Impacta somente o próprio processo levemente	2 - Leve
	De carácter interno – Dentro da área	Até 0,1% da receita líquida	Perturbações muito leves	Não há impacto	1 - Insignificante

Tabela 2: Critérios para a avaliação do Impacto

6.4 A partir do resultado da AGR, os riscos devem ser priorizados pela Administração, a partir de técnicas aplicadas, definindo-se assim aqueles que terão tratamento (Plano de Resposta) e serão acompanhados pela GRC-RCP e pelos órgãos de Governança.

6.4.1 A eficácia da implementação dos planos de resposta aos riscos estratégicos será verificada pela Diretoria Executiva por ocasião do final de ciclo de cada AGR.

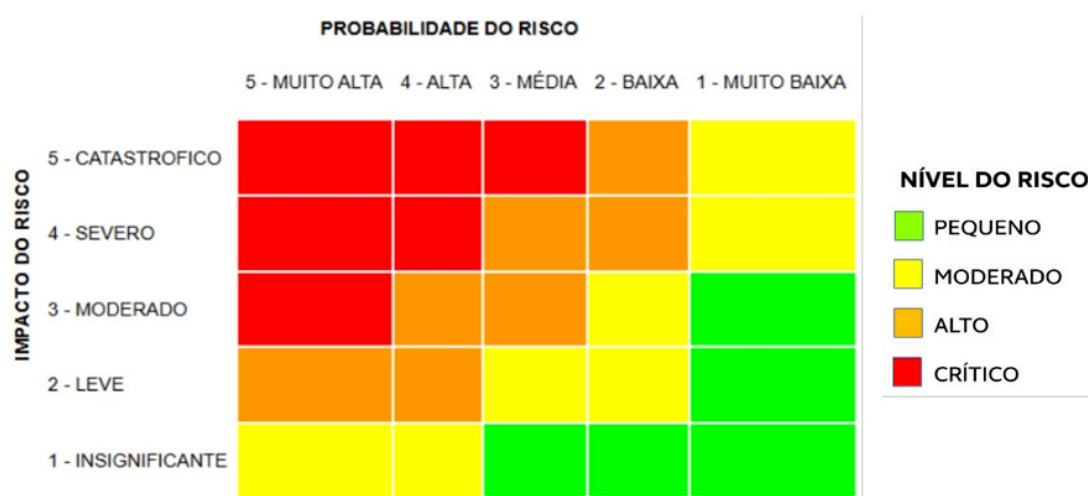


Figura 2: Mapa de Riscos

6.5 Na avaliação dos riscos de processo operacionais, todos os riscos de nível alto e crítico devem ser tratados, com prazos dos planos de resposta estabelecidos no momento da homologação do Plano de Risco, sendo acompanhados pela GRC-RCP.

6.5.1 O planejamento do tratamento das respostas aos riscos deve incluir a análise de diferentes cenários, a avaliação dos aspectos positivos e negativos, a identificação de riscos inter-relacionados e a mensuração da relação entre o impacto do risco e a eficácia da mitigação proposta.

6.5.2 A eficácia da implementação dos planos de resposta aos riscos operacionais será verificada pela respectiva superintendência.

6.6 O Mapa de Riscos é graduado em quatro níveis, definidos em uma matriz, considerando impacto e probabilidade, conforme apresentado na Figura 2.

7. RESPONSABILIDADES

7.1 A Gestão de Riscos Corporativos na Cagece é orientada pela Gerência de Governança, Riscos e Conformidade – GRC, tendo as ações coordenadas pelo Comitê de Gestão de Riscos Corporativos;

7.2 Na Cagece, o Modelo das três Linhas tem como objetivo indicar como as estruturas de gestão e processos se relacionam, auxiliam no alcance dos objetivos e facilitam o gerenciamento de riscos. As linhas estão assim definidas:

7.2.1 Administração: Conselho de Administração, Conselho Fiscal, Diretoria Executiva e Comitê de Auditoria Estatutário

7.2.1.1 Incentiva a cultura que promove comportamento ético e de responsabilidade;

7.2.1.2 Estabelece estruturas e processos para governança;

7.2.1.3 Monitora a gestão e estabelece o direcionamento estratégico

7.2.1.4 Envolve as partes interessadas para monitorar seus interesses e se comunica de forma transparente sobre o atingimento dos objetivos;

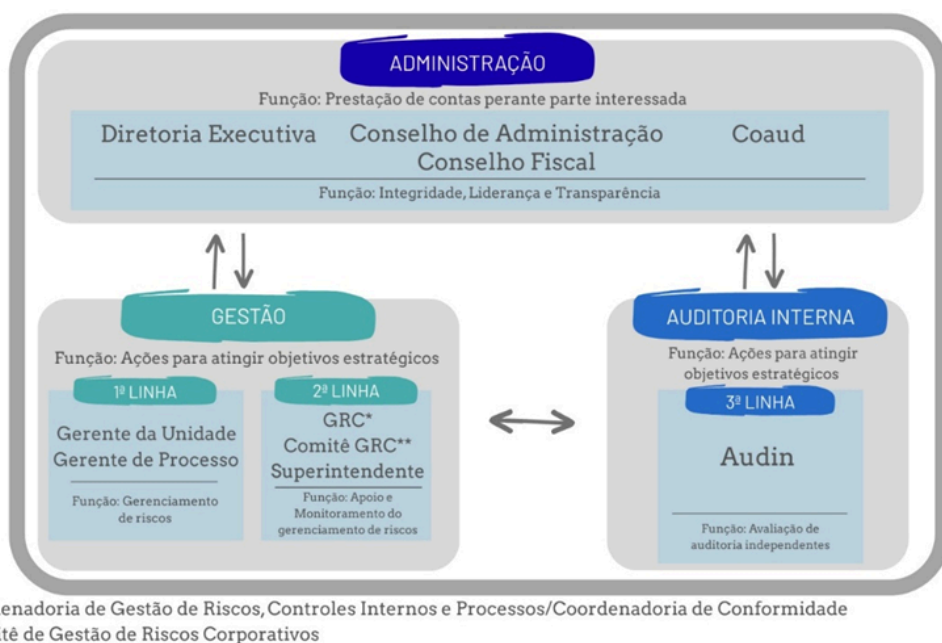


Figura 3: Modelo das Três Linhas

7.2.1.5 Delega responsabilidades e oferece recursos à gestão para atingir os objetivos da organização;

7.2.1.6 Determina o apetite organizacional a riscos e exerce supervisão do gerenciamento de riscos

7.2.1.7 Estabelece e supervisiona a função de auditoria interna independente, objetiva e competente.

7.2.2 Gestão – Primeira linha: Gerente do processo

7.2.2.1 Lidera, dirige ações (incluindo gestão de riscos) e aplica recursos para atingir os objetivos da organização;

7.2.2.2 Mantém diálogo contínuo com a Administração para reportar resultados quanto aos objetivos da organização e a gestão de riscos;

7.2.2.3 Estabelece e mantém estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno);

7.2.2.4 Garante a conformidade com as expectativas legais, regulatórias e éticas.

7.2.3 Gestão – Segunda linha: Gerência de Governança, Riscos e Conformidade (Coordenadoria de Riscos, Controles Internos e processos e Coordenadoria de Conformidade), Comitê de Gestão de Riscos Corporativos e Superintendências.

7.2.3.1 Fornece “expertise” complementar, apoio e monitoramento quanto ao gerenciamento de riscos, incluindo:

7.2.3.1.1 Atual no desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno);

7.2.3.1.2 Busca o atingimento dos objetivos de gerenciamento de riscos.

7.2.3.1.3 Fornece análises e reportes sobre a adequação e eficácia do gerenciamento de riscos.

7.2.4 Auditoria Interna – Terceira linha: Auditoria interna (Audin)

7.2.4.1 Mantém prestação de contas primária perante a Administração e a independência das responsabilidades da gestão;

7.2.4.2 Realiza e comunica sobre avaliação e assessoria independentes à Gestão e à Administração sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua;

7.3 Os riscos corporativos devem ser supervisionados pela Diretoria Executiva, Comitê de Auditoria Estatutário e Conselho de Administração, por meio de relatórios produzidos pela GRC, com periodicidade anual, ou sempre que for solicitado pelos órgãos da administração.

7.4 Aos profissionais da GRC-RCP é permitido o acesso a dados, documentos e informações necessários à execução de suas atividades, responsabilizando-se pela confidencialidade das informações.

7.5 As exceções, eventuais disposições e casos omissos a esta política devem ser submetidas à apreciação do Comitê de Gestão de Riscos Corporativos e encaminhados para posterior aprovação do Conselho de Administração.

8. VIGÊNCIA

8.1 Esta Política Institucional entra em vigor a partir de 27/04/2026, data de aprovação pelo Conselho de Administração da Cagece, conforme Ata nº 693ª .

9. ANEXOS

9.1 Matriz de responsabilidades

9.2 Relação Objetivos Estratégicos (PE 2026-2030) X Macroprocessos

10. HISTÓRICO DE ALTERAÇÕES

Revisão	Elaborador/Unidade	Revisor/Unidade	Aprovador/Unidade	Alterações	Data da Homologação
006	Joana Cordeiro/ GRC-RCP	Michele Aguiar /GRC	CAD	Inclusão da Figura 1 - Modelo de Gestão de Riscos da Cagece Adequação de formato dos itens 2.1 ao 2.7; Ajuste de numeração dos itens :3.4 a 3.32 Ajuste de texto dos itens 5.3 ,5.6, 5.7 ,5.11 Substituição da Tabela 1 - Probabilidade; Ajuste e inclusão dos itens :6.2 a 6.6 Figura 3 Modelo das Três Linhas-Ajuste na numeração e inclusão do Conselho Fiscal para compatibilizar com a Matriz RACI Mudança dos anexos I e II	27/04/2026
005	Joana Cordeiro/ GRC-RCP	Michele Aguiar /GRC	CAD	Itens: 1.2,2, 3.2 , 3.3, 3.4 3.5 , alteração de numeração a partir do item 3.6 em função de inclusão de novos itens. Exclusão do anexo estrutura de riscos/categoria.	26/03/2025
004	Joana Cordeiro/ GRC-RCP Gislene Ellery/ GRC-RCP	Michele Aguiar /GRC	CAD	Anexos II e III	24/03/2023
003	Joana Cordeiro/ GRC-RCP Gislene Ellery/ GRC-RCP	Michele Aguiar /GRC	CAD	Itens: 1, 2, 3, 4, 5, 6, 7, Figura 1, Figura 2, Anexos I, II e III	29/09/2022
002	Gislene Ellery/ GRC-RCP	Michele Aguiar /GRC	-	Itens: 1, 3, 5, 6.2, 6.7, 6.8, 6.9, 6.12, 6.14, Figura 1, Figura 2, 6.15, Figura3, 6.16, 7, Anexo I, Anexo II.	27/07/2020
001	Gislene Ellery/ GRC-RCP	Simone Arrais/GRC	-	-	22/10/2018

ANEXO I – MATRIZ DE RESPONSABILIDADES

A matriz a seguir especifica os papéis e responsabilidades no processo de Gestão de Riscos Corporativos na Cagece através da distribuição das seguintes funções:

R – Responsável (Executa a atividade)

A – Aprovador (Aprova a atividade. Responsável primário pelos resultados)

C – Consultado (Consultado sobre a atividade)

I – Informado (Informado sobre a atividade)

As responsabilidades foram divididas entre os seguintes agentes:

Primeira Linha

- Gestores das áreas de negócios

Segunda Linha

- Coordenadoria de Gestão de Riscos, Controles Internos e Processos (GRC-RCP)
- Coordenadoria de Conformidade (GRC-CON)
- Comitê de Gestão de Riscos Corporativos (CGRC)
- Superintendentes

Terceira Linha

- Auditoria Interna

Administração

- Diretoria Executiva (DE)
- Conselho de Administração (CAD)
- Conselho Fiscal (CF)
- Comitê de Auditoria Estatutário (COAUD)

Atividades		Gestão					Auditoria Interna	Administração				Observação
		1ª linha	2ª linha				3ª linha					
		Gerente de processo	GRC-RCP	GRC-CON	CGRC	Superint.	Audin	Diretoria Executiva	CAD	CF	COAUD	
1. RISCOS ESTRATÉGICOS	1.1 Definição do Apetite ao risco	I	R	I	R	I	I	A	A	I	I	Aprovar o grau de apetite a risco
	1.2 Planejamento e Elaboração da AGR – Análise Geral de Riscos	C	R	C	R	C	I	R	A	I	I	Os ciclos de Análise Geral de Riscos devem ocorrer, no mínimo, a cada 2 anos, ou a partir de decisão da Diretoria Executiva ou Conselho de Administração.
	1.3 Priorização dos Riscos a serem Tratados e acompanhados pela Administração	I	R	I	R	I	I	A	A	I	I	A GRC e o Comitê de Gestão de Riscos propõem um modelo de priorização a ser submetido a aprovação da Diretoria Executiva e do CAD
	1.4 Definição do Tratamento dos Riscos Priorizados (Elaboração e implementação do Plano de Ação)	R	I	I	I	R	I	I	I	I	I	Os articuladores de cada risco priorizado, de acordo com o apetite a riscos da Companhia, devem ser definidos dentre as características necessárias para realizar o tratamento dos referidos riscos.

	1.5 Definir KRI's - Key Risk Indicator (Indicadores chave de risco)	R	C	I	I	R	I	I	I	I	I	Os KRIs devem ser definidos considerando elementos como as causas, o impacto dos riscos e/ou a efetividade dos planos de resposta. A GRC-RCP, no âmbito de suas atribuições, poderá dar suporte as áreas especialistas para definição do KRI's.
	1.6 Monitoramento das ações de tratamento	R	R	R	C	R	I	R	R	R	R	Os riscos selecionados como prioritários terão indicadores a serem monitorados de maneira periódica pela GRC, Diretoria, Conselho de Administração, Conselho Fiscal e Coaud (todos pela GRC-RCP e também pela GRC-CON quando tratar-se de riscos de compliance).O monitoramento dos riscos devem ocorrer: 1. Através de Indicadores de risco (KRI) para os riscos priorizados pela alta administração e para os riscos operacionais de nível crítico; 2 Pelo acompanhamento dos planos de resposta aos riscos.
2. RISCOS OPERACIONAIS	2.1 Identificação e análise dos riscos	R	C	I	I	I	I	I	-	-	-	Eventualmente, os diretores podem ser consultados durante a atividade de identificação dos riscos nos processos.
	2.2 Monitoramento dos riscos de nível moderado e pequeno	R	C	I	I	I	I	I	-	-	-	A primeira linha deverá estar atenta as mudanças no contexto que alterem o nível

												de criticidade dos riscos pequenos e moderados.
	2.3 Definição do tratamento dos riscos com nível alto e crítico (Elaboração e implementação do Plano de Ação)	R	C	I	I	C	I	I	-	-	-	Os planos de resposta aos riscos devem contemplar as ações para redução da probabilidade e/ou mitigação do impacto.
	2.4 Monitoramento das ações de tratamento	R	R	R	I	A	I	I	-	-	-	O Superintendente deverá realizar a verificação de eficácia ao final da implementação dos tratamentos (planos de resposta/ação).
3. COMUNICAÇÃO	3.1 Reporte dos riscos priorizados, com tratamento em andamento	C	R	R	I	I	I	I	I	I	I	Semestral para riscos estratégicos e anual para riscos operacionais.
	3.2 Revisão da política de gestão de riscos	I	R	C	R	I	I	A	A	I	I	A revisão deve ser realizada a cada dois anos, ou a qualquer tempo, se houver necessidade.
4. DISCORDÂNCIA DE OPINIÕES	4.1 Deliberação sobre discordâncias na avaliação e/ou sobre o plano de resposta para riscos estratégicos priorizados	C	R	I	R	C	I	A	A	I	I	A diretoria executiva será acionada para eventuais pontos de discordância entre a GRC-RCP e o Comitê de Gestão de Riscos Corporativos sobre a avaliação e/ ou sobre o plano de resposta para riscos estratégicos. O CAD só será acionado para

												eventuais pontos de discordância entre o Comitê Gestão de Riscos Corporativos e a Diretoria Executiva.
	4.2 Deliberação sobre discordâncias na avaliação e/ou sobre o plano de resposta para riscos operacionais de nível alto ou crítico	C	R	I	R	A	I	A	-	-	-	A Superintendência será acionada para eventuais pontos de discordância entre a GRC-RCP e o Comitê de Gestão de Riscos sobre a avaliação e/ ou sobre o plano de resposta para riscos operacionais. A Diretoria da área só será acionada para eventuais pontos de discordância entre o Comitê Gestão de Riscos Corporativos e a Superintendência.

ANEXO 2 – RELAÇÃO OBJETIVOS ESTRATÉGICOS (PLANO DE GESTÃO ESTRATÉGICA E DE NEGÓCIOS 2026-2030) X MACROPROCESSOS

Perspectiva Econômico-Financeira

Garantir o Crescimento Sustentável

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto
- Gestão de empreendimentos
- Cadastro, faturamento, arrecadação e cobrança
- Concessão e regulação
- Controle da qualidade de produtos
- Gestão de perdas
- Manutenção de sistemas de água e esgoto
- Planejamento e Controle Orçamentário
- Planejamento e controle de vendas
- Relações com as partes interessadas
- Gestão de ativos
- Medição
- Gestão financeira e contábil
- Gestão de eficiência energética
- Gestão socioambiental
- Pesquisa e desenvolvimento

Perspectiva Sustentabilidade

Fortalecer as práticas ambiental, social e governança

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto
- Gestão de empreendimentos
- Relacionamento com clientes
- Concessão e regulação
- Controle da qualidades de produtos
- Gestão de perdas
- Manutenção de sistemas de água e esgoto
- Governança, riscos e conformidade
- Desenvolvimento Empresarial
- Relações com as partes interessadas
- Gestão estratégica de pessoas
- Medição
- Gestão de eficiência energética
- Gestão socioambiental
- Pesquisa e desenvolvimento

ANEXO 2 – RELAÇÃO OBJETIVOS ESTRATÉGICOS (PLANO DE GESTÃO ESTRATÉGICA E DE NEGÓCIOS 2026-2030) X MACROPROCESSOS

Perspectiva Mercado

Assegurar a satisfação do Cliente e melhorar a imagem institucional

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto
- Gestão de empreendimentos
- Cadastro, faturamento, arrecadação e cobrança
- Concessão e regulação
- Controle da qualidade de produtos
- Gestão de perdas

- Manutenção de sistemas de água e esgoto
- Medição
- Relacionamento com clientes
- Planejamento e controle de vendas
- Relações com as partes interessadas
- Gestão de suprimentos
- Gestão de processos jurídicos

- Gestão da TIC
- Gestão Estratégica de pessoas
- Governança, riscos e conformidade
- Gestão da infraestrutura administrativa
- Gestão socioambiental

Universalizar os serviços de Água e Esgoto

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto

- Gestão de empreendimentos
- Cadastro, faturamento, arrecadação e cobrança

- Concessão e regulação
- Gestão de suprimentos

Promover a atuação em novos negócios

- Novos negócios

ANEXO 2 – RELAÇÃO OBJETIVOS ESTRATÉGICOS (PLANO DE GESTÃO ESTRATÉGICA E DE NEGÓCIOS 2026-2030) X MACROPROCESSOS

Perspectiva Processos

Assegurar a qualidade e a continuidade dos produtos e serviços

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto
- Gestão de empreendimentos
- Cadastro, faturamento, arrecadação e cobrança
- Concessão e regulação
- Controle da qualidade de produtos
- Gestão de perdas
- Manutenção de sistemas de água e esgoto
- Medição
- Gestão de suprimentos
- Auditoria Interna
- Gestão de Ativos
- Gestão da TIC
- Gestão Estratégica de Pessoas
- Gestão da infraestrutura administrativa
- Gestão eficiência energética
- Pesquisa e desenvolvimento

Promover inovação e a efetividade dos processos

- Captação, tratamento e distribuição de água
- Coleta, tratamento e disposição de esgoto
- Gestão de empreendimentos
- Concessão e regulação
- Controle da qualidade de produtos
- Gestão de perdas
- Manutenção de sistemas de água e esgoto
- Medição
- Gestão de ativos
- Gestão da TIC
- Gestão estratégica de pessoas
- Governança, riscos e conformidade
- Planejamento e controle orçamentário
- Gestão da infraestrutura administrativa
- Gestão financeira e contábil
- Gestão eficiência energética
- Pesquisa e desenvolvimento

ANEXO 2 – RELAÇÃO OBJETIVOS ESTRATÉGICOS (PLANO DE GESTÃO ESTRATÉGICA E DE NEGÓCIOS 2026-2030) X MACROPROCESSOS

Perspectiva Processos

Reduzir perdas de água

- Captação, tratamento e distribuição de água
- Gestão de empreendimentos
- Cadastro, faturamento, arrecadação e cobrança
- Concessão e regulação
- Gestão de perdas
- Manutenção de sistemas de água e esgoto
- Medição
- Gestão de suprimentos
- Pesquisa e desenvolvimento

Aprimorar a gestão das concessões, empreendimentos e contratos

- Gestão de empreendimentos
- Concessão e regulação
- Gestão de processos jurídicos

Perspectiva Pessoas

Assegurar a valorização dos colaboradores

- Gestão estratégica de pessoas
- Gestão da infraestrutura administrativa

Promover a cultura para gestão para resultados

- Planejamento e controle orçamentário
- Gestão estratégica de pessoas
- Desenvolvimento empresarial