



## DIAGNÓSTICO DE MATURIDADE DA GESTÃO DE RISCOS DA COMPANHIA DE ÁGUA E ESGOTO DO CEARÁ - CAGECE

Relatório técnico apresentado pela mestranda Maríllia Gabrielly Dantas de Moraes ao Programa de Mestrado Profissional em Administração Pública em Rede, sob a orientação do professor Dr. Álvaro Fabiano Pereira de Macedo, como requisito parcial à obtenção do título de Mestre em Administração Pública.

Mossoró  
2023

## Diagnóstico da maturidade da gestão de riscos da Cagece

### Contextualização

O diagnóstico desenvolvido neste relatório técnico tem como objetivo identificar o nível de maturidade da gestão de riscos que vem sendo desenvolvida na Companhia de Água e Esgoto do Ceará (Cagece) e ainda, de acordo com o resultado encontrado, sugerir mudanças por meio de um plano de ação.

Este diagnóstico se justifica, uma vez que é de fundamental importância conhecer e entender em qual nível a gestão de riscos da empresa se encontra para validar e estimular o investimento em ações nesta área. Também se justifica, pois as gestoras de riscos entrevistadas neste estudo expressaram o desejo da realização desta análise, já que em outubro de 2023 a implementação da Política de Gestão de Riscos completará cinco anos e será interessante contar com esta informação de forma documentada.

É importante esclarecer que a Cagece faz parte da Administração Pública Indireta, como Sociedade de Economia Mista Estadual. A Companhia foi criada, conforme informado em seu site oficial, em 1971, com a finalidade de prestar serviços de abastecimento de água, coleta e tratamento de esgoto no Estado do Ceará. O Relatório da Administração da Cagece informa também que a empresa é responsável pelo abastecimento de água em 152 municípios, dos 184 que compõem o Ceará, e pelo esgotamento sanitário de 80 deles, atendendo mais de 5,59 milhões de habitantes (CAGECE, 2023).

Para a realização deste relatório foram utilizadas informações analisadas no decorrer da pesquisa e de dados captados na análise documental. A entrevista foi realizada com três gestoras de riscos da Cagece. Foi empregada a metodologia sugerida pelo Instituto Brasileiro de Governança Corporativa (IBGC, 2017) que consta no caderno intitulado: Gerenciamento de Riscos Corporativos (GRCorp) e, por fim, foi utilizada a ferramenta 5W2H para o plano de ação.

É importante informar que, para o IBGC (2017) a maturidade de riscos representa a compreensão da posição atual da empresa e deve determinar seus objetivos, métodos e meios para alcançá-los. O Instituto explica também que os aspectos que definem a maturidade de riscos em uma organização são: as ações adotadas para o alcance das metas e dos objetivos de gestão de riscos; o nível de

esforço para alcançar essas metas e objetivos; os resultados obtidos, assim como a eficácia e a eficiência das práticas implementadas; o nível de envolvimento dos profissionais relacionado a essas práticas; o nível de entendimento da maturidade da organização, assim como das oportunidades de melhorias.

A metodologia do IBGC propõe a análise de sete componentes e explica que a maturidade de riscos pode ser mensurada por meio de respostas encontradas para reflexões sobre esses componentes. Os componentes sugeridos para a observação são: estratégia de gestão de riscos; governança de gestão de riscos; política de gestão de riscos; processo de gerenciamento de riscos e interação desse processo com os demais ciclos de gestão; linguagem de riscos e métodos de avaliação; sistemas, dados e modelos de informação; cultura de gerenciamento de riscos, comunicação e treinamento e Monitoramento e melhoria contínua (IBGC, 2017).

Cabe mencionar que a Lei Estadual de Acesso à Informação, Lei nº 15.175/2012, mantém em sigilo informações relacionadas à gestão de riscos da Companhia no que se refere, principalmente, a estratégias, classificações e objetivos de gerenciamento. Por este motivo, a análise foi realizada com os documentos disponibilizados em seu site oficial e com as informações fornecidas pelas gestoras lotadas na Gerência de Governança, Risco e Conformidade (GRC) durante entrevista concedida. As gestoras ocupam os cargos de gerente, coordenadora e supervisora

Segue o Quadro 9 que fornece as reflexões feitas sobre cada componente de gestão de riscos. A cada componente foram tecidos comentários que ao final justificam a classificação de maturidade da companhia, conforme definição do IBGC em: inicial, fragmentada, definida, consolidada e otimizada.

**QUADRO 9 – MENSURANDO A MATURIDADE DA GESTÃO DE RISCOS**

	<b>Componente de Gestão de Riscos</b>	<b>Reflexões</b>
1	Estratégia de gestão de riscos	• Existem estratégias, objetivos e metas de gestão de riscos estabelecidos?
2	Governança de gestão de riscos	• Existe estrutura organizacional com papéis e responsabilidades claramente definidos nas práticas de gestão de riscos? • A estrutura considera papel do Conselho de Administração e da diretoria e de todas as três linhas de defesas detalhadas no modelo de governança de gestão de riscos?
3	Política de gestão de riscos	• As questões acima mencionadas estão regimentadas, aprovadas e divulgadas por meio de uma política de gestão de riscos?
4	Processo de gerenciamento de riscos e interação com os demais ciclos de gestão	• Existe processo de gestão de riscos definido e implementado com atividades de identificação de

		<p>riscos, avaliação de riscos, avaliação das atividades de controle, resposta, monitoramento e comunicação?</p> <ul style="list-style-type: none"> <li>• Existe norma de gestão de riscos (ou documento equivalente), de divulgação interna, que estabelece procedimentos, responsabilidades, segregação de funções, fronteiras de atuação e o sistema geral de governança da gestão de riscos?</li> <li>• As práticas de gestão de riscos estão alinhadas às demais práticas de controle?</li> <li>• Existe um modelo definido para a incorporação do gerenciamento de riscos nos processos decisórios e nos ciclos de gestão?</li> </ul>
5	Linguagem de riscos e métodos de avaliação	<ul style="list-style-type: none"> <li>• Existe taxonomia de riscos (categorias) e métodos de avaliações definidos?</li> <li>• A organização utiliza-se de técnicas de mensuração?</li> </ul>
6	Sistemas, dados e modelos de informação	<ul style="list-style-type: none"> <li>• As informações sobre a exposição de riscos da organização são compartilhadas com os diferentes níveis da organização e capturadas de forma consistente?</li> </ul>
7	Cultura de gerenciamento de riscos, comunicação e treinamento e monitoramento e melhoria contínua	<ul style="list-style-type: none"> <li>• O gerenciamento de riscos está incorporado no processo decisório, na cultura da organização e no dia a dia da gestão do negócio?</li> <li>• A organização avalia o entendimento dos empregados em relação à cultura, às práticas de gestão de riscos e ao sistema de controles internos?</li> <li>• As ações de comunicação e treinamento da cultura de gestão de riscos são realizadas com os diferentes públicos da organização?</li> <li>• Os órgãos de governança e as três linhas de defesa monitoram permanentemente as práticas de gestão de riscos?</li> <li>• O gerenciamento de riscos é realizado de forma contínua?</li> </ul>

Fonte: Adaptado de IBGC, 2017

### 1.1.1 Estratégia de gestão de riscos

A primeira reflexão sugerida pelo IBGC é relacionada à estratégia, aos objetivos e às metas de gestão de riscos. Sobre estes pontos, as gestoras mencionaram a preocupação da gestão da Cagece em estabelecer as estratégias de riscos e fazê-la de forma clara para ser disseminada por toda a organização. Complementando a afirmação das entrevistadas, o Estatuto Social da empresa explica em seu artigo 17, inciso XXIV, que o Conselho de Administração (CAD) deve aprovar o planejamento estratégico, contendo a estratégia de longo prazo atualizada com análise de riscos e oportunidades para, no mínimo, os próximos 5 (cinco) anos, as diretrizes de ação, metas de resultado e índices de avaliação de desempenho.

Sobre os objetivos, a Carta Anual de Políticas Públicas informa o crescimento de ações para disseminar a gestão de riscos e consolidá-la como uma ferramenta importante para o atingimento dos objetivos do negócio e execução das políticas públicas, ficando clara a importância crescente dada à temática na empresa. Ainda como exemplo de estabelecimento de objetivos baseados no gerenciamento de riscos, o Relatório de Sustentabilidade da Companhia, publicado em 2021, relata que:

Em 2020, foi atualizada a Análise Geral de Riscos (AGR), pela qual todos os riscos da Companhia são avaliados e analisados quanto à probabilidade e impacto. A partir da avaliação final, a Cagece apresentou 9 riscos com nível crítico, dentre os quais, três relacionados à sub-categoria resíduos, emissões e efluentes. Como Plano de Resposta para esses e outros riscos relacionados ao meio ambiente, foi concebido o Programa de Qualidade dos Produtos Água e Esgoto (PQAE). Trata-se de um programa de longo prazo (2021-2035) que tem como objetivo implantar ações estratégicas para que os indicadores de qualidade de água e esgoto alcancem os padrões de qualidade estabelecidos em Lei (RELATÓRIO DE SUSTENTABILIDADE, 2021).

Nos documentos disponíveis para a análise é possível identificar passagens, como estas citadas, que remetem ao estabelecimento tanto de objetivos como de metas. Contudo, por estes temas estarem protegidos pelo sigilo imposto pela Lei 15.175/2012, não há como especificá-los objetivamente. Apesar do impedimento, ainda é possível observar que eles existem e estão presentes nos documentos e nas falas das gestoras entrevistadas neste estudo.

### **1.1.2 Governança de gestão de riscos**

Passando para a análise do segundo item de reflexão que trata da governança, é possível apontar de forma mais clara os questionamentos anunciados. Sobre a definição dos papéis e responsabilidades nas práticas de gerenciamento de riscos, em seu Relatório de Sustentabilidade define-se que as responsabilidades de elaboração e condução do processo de gestão de riscos na Cagece foram divididas entre os agentes que compõem: a Coordenadoria de Gestão de Riscos Controles Internos e Processos (GRC-RCP); os Gestores das Áreas de Negócios; o Comitê de Gestão de Riscos Corporativos (CGRC); a Diretoria Executiva (DE); e o Conselho de Administração (CAD).

Além disso, fica claro o entendimento da estrutura mencionada no parágrafo anterior, uma vez que a Política de Gestão de Riscos define essa divisão de responsabilidades dentro da estrutura do Modelo das Três Linhas. Nessa estrutura, a Primeira Linha corresponde aos Gestores das áreas de negócios; a Segunda Linha conta com a Coordenadoria de Gestão de Riscos, Controles Internos e Processos, com o Comitê de Gestão de Riscos Corporativos e com os Superintendentes; já na Terceira Linha está a Auditoria Interna; e por fim, compondo a Administração estão a Diretoria Executiva e o Conselho de Administração.

As categorias especificadas recebem funções classificadas em: responsável (executa a atividade); aprovador (aprova a atividade; é responsável primário pelos resultados); consultado (é consultado sobre a atividade); informado (é informado sobre a atividade); supervisor (supervisiona a atividade). No Anexo I da Políticas são então especificadas as atividades a serem realizadas, que vão de tarefas de planejamento, mapeamento de riscos e planos de respostas até os reportes periódicos e o monitoramento contínuo dos riscos. Com essas atividades bem definidas, são feitas as distribuições de funções para cada grupo com a obrigação que pode ser de responsável a supervisor, de acordo com a tarefa.

A maioria dos documentos disponibilizados no site remetem a essa estrutura organizacional de forma clara e segura, assim como também é possível identificar nas falas das entrevistadas, a naturalidade na definição das responsabilidades, até mesmo quando remetem aos demais empregados que já identificam de forma objetiva os envolvidos nas tarefas essenciais às suas áreas de trabalho.

### **1.1.3 Política de gestão de riscos**

A terceira reflexão sugerida pelo IBGC tem como foco principal a Política de Gestão de Riscos e, sobre ela, repercutindo os tópicos mencionados anteriormente. Nesse contexto, fica claro observar tanto os itens referentes à estratégia e aos objetivos quanto aos que mencionam a governança e sua estrutura com divisão de responsabilidades.

É importante mencionar que a Política da Companhia engloba assuntos que contextualizam os riscos na dinâmica organizacional, definindo e explicando conceitos essenciais ao entendimento da temática. Passa pelos seus objetivos, diretrizes e

princípios, deixando-os claros para não desviarem do que a Companhia percebe e imagina em seus cenários. E contempla, também, as principais características e responsabilidades dos setores e gestores determinados à execução das atividades necessárias para a implementação e execução da política.

A Política de Gestão de Riscos da Cagece é clara e objetiva em todas as suas subdivisões, fazendo com que tanto o seu público interno quanto o externo tenham noção das suas principais características. Ela também conta com um histórico das alterações realizadas pela GRC que aconteceram em 2020, 2022 e 2023, demonstrando a preocupação em atualizar ou modificar algo que já não faz mais sentido para a organização.

Pelos motivos elencados, é possível concluir que a Política contempla todos os pontos, uma vez que atende aos questionamentos requisitados pela metodologia a que este trabalho se submete.

#### **1.1.4 Processo de gerenciamento de riscos e interação com os demais ciclos de gestão**

O quarto tópico abordado pela metodologia do IBGC leva em consideração o processo de gerenciamento de riscos. A primeira reflexão diz respeito às atividades de identificação, avaliação, controle, resposta, monitoramento e comunicação de riscos. Sobre elas é interessante abordar que acontecem na organização e tem grupos de trabalho (GTs) em cada área definida pela gestão para definirem e tratarem os riscos que são considerados críticos, conforme mencionado pelas gestoras ouvidas por esta pesquisa.

A Política de Gestão de Riscos define o processo de gestão de riscos trazendo os tópicos mencionados no parágrafo anterior e observando que eles são capazes de afetar o alcance dos objetivos da Cagece. É de responsabilidade da GRC promover uma ampla discussão com as áreas para desenvolver esse processo de gestão de riscos. A política também explica que suas bases são compostas pelo COSO ERM, pelas normas ABNT NBR ISO 31000, ABNT ISO GUIA 73 e o Modelo das Três Linhas do Instituto de Auditores Internos do Brasil – IIA Brasil.

Já sobre o questionamento da divulgação interna com o estabelecimento de responsabilidades, é importante falar sobre o Programa de Disseminação da

Metodologia de Gestão de Riscos, Controles Internos e Processos que envolve toda a organização e busca levar informações para os empregados. Estes passam a entender além dos conceitos estabelecidos e dos procedimentos a serem adotados, e começam a contribuir com as metas de mapeamento de processos e de realização da gestão de riscos, que possuem prazos em 2023 e 2024 para toda a Companhia.

Com a análise documental é possível perceber também a integração da gestão de riscos com as demais práticas da Companhia, tanto as que lidam com os controles internos, como por exemplo as Auditorias internas e externas, quanto nos objetivos de outras áreas, uma vez que seus objetivos atingem suas estruturas estratégica, financeira e operacional, demonstrando alinhamento e conexão na organização como um todo.

A última reflexão sugerida para esta etapa refere-se à incorporação da gestão de riscos nos processos decisórios. Na entrevista foi possível perceber o desejo das gestoras em fazer da gestão de riscos uma ferramenta potente para o auxílio nas tomadas de decisões, fazendo com que ela subsidie de forma objetiva essas escolhas por parte dos gestores. Porém, elas salientaram que a situação abordada ainda não acontece de forma efetiva, apesar de estar evoluindo a cada novo ciclo de avaliação e acreditarem que vai acontecer em breve.

### **1.1.5 Linguagem de riscos e métodos de avaliação**

O quinto ponto de observação reflete sobre as categorias de riscos, métodos de definição e técnicas de mensuração. Sobre este assunto pode-se depreender que há categorias bem definidas dos riscos na Companhia e eles são classificados no documento nomeado de Dicionário de Riscos. Esse dicionário divide os riscos em: Estratégicos; Financeiros; Operacionais; e Legais.

Os riscos estratégicos são subdivididos em três áreas. A área de Governança possui riscos relacionados a: conformidade; conduta ética; reputação e imagem; relacionamento com acionistas; e estrutura organizacional. Já a área de Modelo de Negócios pode conter riscos de: planejamento estratégico; planejamento orçamentário; inovação e tecnologia; investimento em projetos; continuidade dos negócios; satisfação do Cliente; mercado e concorrência; e parcerias. Por fim, a área classificada em Política e Econômica possui riscos no cenário político e econômico.



Os riscos financeiros também são divididos em três áreas. A área classificada em Crédito é relacionada com: inadimplência; e concentração. A de Mercado integra possíveis riscos relacionados a: taxas de juros; câmbio; e financiamentos. A última área de riscos financeiros é a de Liquidez e engloba riscos de fluxo de caixa.

Os riscos operacionais subdividem-se em cinco áreas, cada uma refletindo mais divisões de riscos. A de Processo abarca os riscos de capacidade operacional e eficiência no desenvolvimento de processos; os riscos de fornecimento; e os referentes a perda e/ou obsolescência. Já a área Pessoal contém a preocupação com riscos de capacitação; retenção de talentos; e saúde e segurança. Na área de Tecnologia da Informação os riscos prevalentes relacionam-se à segurança da informação; e disponibilidade de infraestrutura. As duas últimas áreas dos riscos operacionais são relacionadas a Informações, contendo o risco da integridade das informações e, por fim, a área relacionada ao Meio Ambiente que contém os riscos de resíduos, emissões e efluentes.

A última categoria de riscos denominada de riscos legais é subdividida em quatro tipos principais de riscos que são: trabalhistas; tributários; cíveis; e conformidade regulatória.

Sobre a técnica de mensuração, a Cagece realiza a Análise Geral de Riscos (AGR), pela qual todos os riscos da Companhia são avaliados e analisados quanto à probabilidade e ao impacto. Neste critério, cruzando as análises da probabilidade que levam em conta, por exemplo, se o grau de exposição é diário, quinzenal, mensal, anual ou eventual, e analisando também o se o impacto é nacional, regional ou interno, por exemplo, os riscos são divididos em quatro níveis classificáveis em: pequeno, moderado, alto e crítico.

Conforme exposto na Política de Gestão de Riscos da Companhia, a Coordenação de Riscos e Controles Internos e o Comitê de Riscos Corporativos são responsáveis por executar a definição do grau de tolerância do risco (apetite ao risco), avaliação e priorização dos riscos identificados. O Conselho de Administração (CAD) é o órgão responsável por aprovar e monitorar todo o material desenvolvido, e apoiar a implementação dos sistemas de gestão de riscos e de controles internos. A Política estabelece em uma Matriz de Responsabilidades a atuação do CAD quanto às responsabilidades de aprovação, recepção de informações e assessoramento para disponibilizar ou orientar sobre como tratar as informações. Nessa Matriz são

contempladas atividades de análise de riscos, apetite ao risco, avaliação e priorização aos riscos e plano de respostas ao risco (CAGECE, 2022).

Diante das discriminações e respostas às reflexões, fica claro o atendimento da Cagece às especificações propostas, demonstrando, portanto, o cumprimento deste quinto ponto de observação de forma satisfatória.

#### **1.1.6 Sistemas, dados e modelos de informação**

A sexta reflexão sugerida pela metodologia do IBGC traz à tona o questionamento sobre a possibilidade de levar aos diferentes níveis da empresa informações sobre a exposição de riscos de cada área. Sobre este assunto foi possível perceber, durante a entrevista realizada com as gestoras, que há uma preocupação da Companhia para que os dados relacionados ao gerenciamento de riscos cheguem a todos os empregados.

Nesta perspectiva, treinamentos e fóruns são realizados e abertos para todos que fazem parte da empresa. O objetivo principal é a sensibilização sobre o impacto do tema para a Cagece, para que os envolvidos possam entender a temática, sendo capazes também de perceber e opinar sobre o assunto, enriquecendo as discussões e possibilitando melhorias. No mesmo sentido, o Programa de Disseminação da Gestão de Riscos, já mencionado anteriormente, também contribui para divulgar e ampliar os conhecimentos sobre riscos, e, segundo a coordenadora da GRC, por meio dele a temática de riscos conseguiu chegar de forma efetiva na base da organização.

As entrevistadas explicaram também que um sistema de gestão de riscos foi adquirido por meio de licitação pela empresa e tem como objetivo, dentre tantos outros, facilitar a visualização e comunicação por parte de todos os níveis da companhia, dada a necessidade de disseminação dessas informações para o sucesso das estratégias de gerenciamento de riscos.

#### **1.1.7 Cultura de gerenciamento de riscos, comunicação e treinamento e monitoramento e melhoria contínua**

O último ponto de reflexão tem como base a cultura organizacional em torno da gestão de riscos e como a comunicação, o treinamento, o monitoramento e a melhoria contínua estão interrelacionados. Dentro desta perspectiva é possível perceber, tanto nos documentos analisados quanto no decorrer da entrevista realizada, que a organização tem passado por um processo de difundir a cultura de gestão de riscos e se preocupa em fazê-lo de forma sistematizada contando com o Programa de Disseminação da Metodologia de Gestão de Riscos, Controles Internos e Processo.

O principal objetivo é levar ao dia a dia dos empregados facilidades e comodidades da gestão de riscos e incorporá-la à rotina das atividades diárias. O Programa de Disseminação da Gestão de Riscos da Companhia tem feito o seu papel neste aspecto e para as gestoras ele tem sido essencial para essa conexão da temática com os diversos níveis e áreas da Companhia.

Dentro deste contexto, a Carta Anual de Políticas Públicas explica que:

Os controles internos e a Gestão de Riscos são fortemente disseminados na Cagece e vêm se consolidando nos últimos anos como ferramentas essenciais para o atingimento dos objetivos do negócio. (...) Na Companhia, a Gestão de Riscos é disseminada em todos os níveis da organização, cabendo ao responsável por cada processo gerenciar os seus respectivos riscos. (...) Treinamentos periódicos são realizados junto ao corpo funcional da Companhia com o objetivo de disseminar a cultura da Gestão de Riscos e de Processos. A Companhia promove a interação entre seus diversos agentes de controle, com vistas a subsidiar o alcance dos objetivos organizacionais, a partir de um sistema orientado para prevenir, detectar e remediar riscos de conformidade e integridade (CAGECE, 2023).

Sobre os treinamentos, a Cagece se preocupa em treinar e atualizar seus empregados de forma contínua e abrangendo toda a organização. A cada mudança na estrutura, os empregados que passam a ocupar cargos de chefia ou a fazer parte do Grupo de Trabalho (GT) para a realização do gerenciamento de riscos, também são orientados pela GRC para realizarem os cursos pré-determinados.

A Alta Administração também passa por um treinamento anual organizado pela GRC, em atendimento à Lei nº 13.303/2016, em que a temática de riscos é discutida. As atualizações legislativas são repassadas e isso leva a uma maior integração dos membros dos Conselhos de Administração, Fiscal, Comitê de Auditoria Estatutário, Diretoria e destes com demais gestores.

O monitoramento das práticas de gerenciamento de riscos por parte da empresa é constante, uma vez que os riscos são mutáveis no decorrer do tempo. A gerente informou que a cada quatro meses, que corresponde ao que é chamado de

ciclo, os riscos são avaliados para analisar se continuam com a mesma classificação ou se a resposta sugerida para eles surtiu efeitos e foi reduzido o seu nível de criticidade. Outro acompanhamento que também existe é a avaliação da Política de Gestão de Riscos a cada dois anos, demonstrando, portanto, a preocupação em atualizar a situação da Companhia para que esteja sempre em capacidade de melhorar seus processos e tarefas diárias.

## 1.2 MENSURAÇÃO DA MATURIDADE COM BASE NOS COMPONENTES DE GESTÃO DE RISCOS DO IBGC

Depois de responder às reflexões sugeridas no tópico anterior, é possível ter uma base concreta para analisar e identificar a maturidade em que a empresa se encontra. A Figura 12 mostra a classificação proposta pelo IBGC e em seguida é exposto o Quadro 10 com a classificação de cada componente baseado nas análises expostas.

FIGURA 12 – MENSURAÇÃO DA MATURIDADE DE GRCORP

	(1) Estratégia de GRCorp	(2) Governança de GRCorp	(3) Política de GRCorp	(4) Processo de GRCorp e Interação do processo de GRCorp com demais ciclos de gestão	(5) Linguagem de riscos e Métodos de avaliações	(6) Sistemas, dados e modelos de informação	(7) Cultura, Comunicação e treinamento, monitoramento e melhoria contínua
<b>OTIMIZADO</b>	<ul style="list-style-type: none"> <li>Estratégia de gestão de riscos claramente definida, implementada e integrada aos demais ciclos de gestão</li> <li>As metas de desempenho estão alinhadas com a estratégia e a gestão de riscos</li> </ul>	<ul style="list-style-type: none"> <li>Os objetivos estão claramente definidos e alinhados entre as diversas funções da 2ª linha de defesa a fim de prover valor para a organização</li> <li>O modelo é referência do setor</li> </ul>	<ul style="list-style-type: none"> <li>Políticas e procedimentos são regularmente referenciados por terceiros e pelo setor. As políticas têm impacto sobre o ambiente de negócios externo</li> </ul>	<ul style="list-style-type: none"> <li>Os processos de identificação e avaliação de riscos estão bem integrados aos objetivos estratégicos</li> <li>Atividades de monitoramento eficientes e coordenadas</li> </ul>	<ul style="list-style-type: none"> <li>Utiliza abordagem padronizada e consistente para definir o apetite e tolerância a riscos</li> <li>Cenários futuros e testes de stress são usados para explorar a análise dos riscos</li> </ul>	<ul style="list-style-type: none"> <li>Tecnologias integradas habilitam a organização a gerenciar os riscos e são consideradas altamente efetivas e reconhecidas como práticas líderes pelo mercado</li> </ul>	<ul style="list-style-type: none"> <li>A cultura de riscos e controles é efetiva em todos os níveis da organização</li> <li>Programas de disseminação são aplicados para a evolução contínua da gestão de riscos</li> </ul>
<b>CONSOLIDADO</b>	<ul style="list-style-type: none"> <li>Estratégia de gestão de riscos claramente definida e implementada</li> <li>As metas de desempenho são monitoradas</li> </ul>	<ul style="list-style-type: none"> <li>As funções da 2ª linha de defesa cobrem os riscos da organização</li> <li>A estrutura organizacional está bem definida e alinhada à estratégia e aos objetivos</li> </ul>	<ul style="list-style-type: none"> <li>Políticas e procedimentos são bem desenvolvidos e aplicados consistentemente em toda a organização</li> <li>São continuamente atualizados de acordo com as mudanças na estratégia de negócios</li> </ul>	<ul style="list-style-type: none"> <li>Os processos de identificação e avaliação de riscos estão bem definidos, estruturados</li> <li>Os gestores de negócio monitoram sistematicamente os riscos associados aos seus processos</li> </ul>	<ul style="list-style-type: none"> <li>Utiliza abordagem padronizada e consistente para definir o apetite e a tolerância a riscos</li> <li>Testes de stress e análise de cenários são utilizados em nível corporativo</li> </ul>	<ul style="list-style-type: none"> <li>Tecnologias emergentes são aproveitadas para permitir que os objetivos de gestão de riscos sejam alcançados em nível corporativo</li> </ul>	<ul style="list-style-type: none"> <li>A cultura de riscos e controles está inserida nas atividades diárias da organização e os riscos são proativamente tratados nos níveis de processo e de funções</li> </ul>
<b>DEFINIDO</b>	<ul style="list-style-type: none"> <li>Estratégia de gestão de riscos claramente definida e implementada</li> <li>As metas de desempenho são definidas</li> </ul>	<ul style="list-style-type: none"> <li>As funções da 2ª linha de defesa cobrem os riscos de negócio e direcionadores de valor, podendo haver sobreposições</li> <li>A estrutura organizacional está definida</li> </ul>	<ul style="list-style-type: none"> <li>Políticas e procedimentos de GRCorp são formais e comunicadas de forma consistente em toda a organização</li> </ul>	<ul style="list-style-type: none"> <li>Uma abordagem baseada em riscos é executada de maneira sistemática e consistentemente aplicada em nível corporativo e por toda a organização</li> </ul>	<ul style="list-style-type: none"> <li>Há uma abordagem padronizada para definir o nível aceitável de riscos. No entanto, ela não é utilizada por todas as funções de maneira consistente</li> </ul>	<ul style="list-style-type: none"> <li>Os modelos de informações e de relatórios são bem definidos e compreendidos. Os relatórios são elaborados com informações corretas, completas</li> </ul>	<ul style="list-style-type: none"> <li>Protocolos claros de comunicação existem e são abertos a todos os empregados. A comunicação de duas mãos com as partes interessadas é incentivada.</li> </ul>
<b>FRAGMENTADO</b>	<ul style="list-style-type: none"> <li>A organização sabe por onde começar, mesmo que não tenha claro aonde quer chegar</li> <li>As metas de desempenho existem</li> </ul>	<ul style="list-style-type: none"> <li>As funções da 2ª linha de defesa focam em áreas históricas em resposta ao cumprimento das obrigações regulatórias</li> </ul>	<ul style="list-style-type: none"> <li>Políticas e procedimentos são limitados a áreas diretoras-chave</li> </ul>	<ul style="list-style-type: none"> <li>Os processos de identificação e avaliação de riscos são executados como atividades distintas ou separadas acontecendo sob demanda</li> </ul>	<ul style="list-style-type: none"> <li>Não há abordagem padronizada para definir o nível aceitável de riscos</li> <li>Análises qualitativas e quantitativas são realizadas</li> </ul>	<ul style="list-style-type: none"> <li>Modelos de informações e relatórios são definidos pela alta direção, mas não são compreendidos pela gestão ou alinhados na organização</li> </ul>	<ul style="list-style-type: none"> <li>Existem comunicações, mas não estão formalmente definidas.</li> <li>Treinamentos pontuais são realizados</li> </ul>
<b>INICIAL</b>	<ul style="list-style-type: none"> <li>A organização não sabe como, quem, quando, onde e por que implementar gestão de riscos</li> <li>As metas de desempenho existem</li> </ul>	<ul style="list-style-type: none"> <li>As funções da 2ª linha de defesa são realizadas individualmente, não integradas à visão estratégica.</li> </ul>	<ul style="list-style-type: none"> <li>Políticas e procedimentos não estão definidos e não há um processo consistente para seu desenvolvimento e manutenção</li> </ul>	<ul style="list-style-type: none"> <li>Processos e controles que dão apoio à gestão de riscos são pouco desenvolvidos</li> <li>Mínimas atividades de monitoramento ocorrem.</li> </ul>	<ul style="list-style-type: none"> <li>Não há abordagem padronizada para definir o nível aceitável de riscos</li> <li>Análises qualitativas e quantitativas são realizadas</li> </ul>	<ul style="list-style-type: none"> <li>Modelos de informações e relatórios são direcionados por exigências externas e não são suficientemente definidos</li> </ul>	<ul style="list-style-type: none"> <li>Não há um plano de disseminação implementado para formalizar as principais decisões da companhia em relação às práticas de riscos</li> </ul>

Fonte: IBGC, 2017

QUADRO 10 – MENSURAÇÃO DA MATURIDADE DA CAGECE

Componentes de GR Corp	Avaliação
Estratégia de gestão de riscos	Otimizada
Governança de gestão de riscos	Otimizada
Política de gestão de riscos	Otimizada
Processo de gerenciamento de riscos e interação com os demais ciclos de gestão	Definido
Linguagem de riscos e métodos de avaliação	Definido
Sistemas, dados e modelos de informação	Definido
Cultura de gerenciamento de riscos, comunicação e treinamento e monitoramento e melhoria contínua	Consolidada

Fonte: Dados da pesquisa, 2023

O IBGC (2017) explica que o objetivo de utilizar o modelo de maturidade é fornecer para a organização um guia que facilite a melhoria na capacidade de gestão, permitindo a definição de uma abordagem realista de curto, médio e longo prazos para a estratégia de Gestão de Riscos. Essa avaliação permite que a organização possa documentar, comunicar e programar melhorias no seu modelo de gerenciamento. O produto final da avaliação deverá compreender a análise da situação atual em cada dimensão, a definição do estágio desejado e as ações requeridas para se alcançar o estágio desejado, que devem ser objeto de planos de ação. É dentro dessa perspectiva que foram realizadas sugestões para os planos de ação percebidos como necessários no tópico a seguir.

### 1.3 PLANO DE AÇÃO

Ainda levando em consideração a metodologia proposta pelo IBGC apresenta-se a situação almejada para a organização em estudo baseado no Quadro 11 estabelecido a seguir:

QUADRO 11 – CONSOLIDAÇÃO DOS RESULTADOS DE MATURIDADE

Dimensão	Nível de Maturidade					Estágio atual	Estágio desejado
	1.Inicial	2.Fragmentado	3.Definido	4.Consolidado	5.Otimizado		
Processo de gerenciamento de riscos e interação com os demais ciclos de gestão			●	→★		3	4
Linguagem de riscos e métodos de avaliação			●	→★		3	4
Sistemas, dados e modelos de informação			●	→★		3	4
Cultura de gerenciamento de riscos, comunicação e					●	→★	5

treinamento e monitoramento e melhoria contínua							
--	--	--	--	--	--	--	--

Fonte: Adaptado de IBGC, 2017

O IBGC (2017) explica que, uma vez analisado o nível de maturidade atual e definido o nível almejado, a empresa deve estabelecer as ações para a evolução das práticas de gestão de riscos, designando um grupo de trabalho para a atuação nos planos estabelecidos.

Com o objetivo de sugerir melhorias para os componentes de gestão de riscos corporativos que não alcançaram a nota máxima na mensuração da maturidade da Cagece, foi realizado um plano de ação, por meio da ferramenta 5W2H, contendo alternativas para que nos próximos ciclos, a maturidade possa melhorar a sua classificação.

Mello et al (2016) definem a ferramenta 5W2H como um plano de ação que tem por objetivo executar um checklist para tornar preciso o resultado que se pretende alcançar realizando perguntas que permitirão, por meio de suas respostas, obter um planejamento geral para a tomada de decisão quanto às ações que devem ser realizadas. Lucinda (2016) complementa que a sigla 5W2H são as iniciais de sete perguntas a serem respondidas com o objetivo de dirimir quaisquer dúvidas sobre o que deve ser feito. 5W e 2H são as iniciais de perguntas em inglês que significam: O quê? (*What?*); Por quê? (*Why?*); Onde? (*Where?*); Quem? (*Who?*); Quando? (*When?*); Como? (*How?*); Quanto? (*How Much?*). Nesse contexto, o próximo tópico apresentará as sugestões propostas.

### 1.3.1 Planos de ação

Plano 1: Melhoria no processo de gerenciamento de riscos e interação com os demais ciclos de gestão

O fator analisado que gerou o rebaixamento na maturidade do componente “processo de gerenciamento de riscos” foi a falta de um modelo que incorpore a gestão de riscos aos processos decisórios da empresa. Nesse sentido, caberá aos gestores elaborarem um diagnóstico que elenque os principais resultados alcançados pela

Companhia e que possam ser associados a práticas de gerenciamento de riscos implementadas de forma objetiva e clara.

O objetivo principal desse diagnóstico institucional é possibilitar o entendimento, por parte dos colaboradores, de que a gestão de riscos não se restringe a um procedimento legal a ser adotado e que ela pode ser fator determinante para uma escolha bem-sucedida que resulta em alcance de metas. Esse processo é lento, pois esbarra em fronteiras culturais da companhia, mas é de fundamental importância para que a gestão de riscos seja percebida como uma ferramenta efetiva. O Quadro 12 a seguir apresenta a proposta elaborada

QUADRO 12 – PLANO DE AÇÃO 1

Diagnóstico Institucional	
<b>5W</b>	
O quê? (What)	Fazer um levantamento associando o gerenciamento de riscos ao alcance de objetivos organizacionais
Por quê? (Why)	Ao associar a gestão de riscos ao atingimento de metas e resultados, a ferramenta se fortalece e passa a ser popularizada frente a decisões de pequeno ou de grande porte
Onde? (Where)	Em todos os níveis hierárquicos da Companhia
Quem? (Who)	Gerência de Governança, Riscos e Conformidade (GRC)
Quando? (When)	Anualmente.
<b>2H</b>	
Como? (How)	Publicação do Diagnóstico Interno Anual que contemple os resultados alcançados pelas áreas, associando a ações realizadas pelos setores, gerando a sensação de pertencimento aos que fazem o gerenciamento de seus riscos.
Quanto? (How Much)	-

Fonte: Dados da pesquisa, 2023

#### Plano 2: Melhoria na linguagem de riscos e métodos de avaliação

Para analisar a possibilidade de melhoria deste componente faz-se necessário informar que seu ponto de dificuldade é relacionado à ausência de prospecção de cenários e ainda ao fato de não existirem testes de estresse relatados tanto nos documentos analisados quanto na fala das entrevistadas.

Com isso, é necessário que a equipe gestora busque conhecimentos para desenvolver essas ações e consiga implementar essa melhoria para a análise dos

seus riscos. Nesse contexto, sugere-se a busca por treinamentos e consequentemente seja colocado em prática por meio de visualizações dos cenários para determinadas escolhas ou ainda os testes de estresse. O Quadro 13 a seguir apresenta a proposta elaborada.

QUADRO 13 – PLANO DE AÇÃO 2

Treinamento e aquisição de software	
5W	
O quê? (What)	Treinar profissionais escolhidos pela GRC para posterior aplicação da teoria na empresa por meio de software a ser adquirido
Por quê? (Why)	Como não houve menção nos documentos e na entrevista sobre a análise de cenários e testes de estresse, já que é um fator importante para a metodologia determinada pelo IBGC, faz-se necessário buscar o conhecimento para que por meio dele sejam propostas e executadas ações futuras de melhorias para a companhia com softwares e treinamentos
Onde? (Where)	Gerência de Governança, Riscos e Conformidade
Quem? (Who)	Profissionais designados para participarem do treinamento e aplicarem ao software
Quando? (When)	Em até dois anos
2H	
Como? (How)	Contratação de profissionais ou curso especializados que ministrem aulas de capacitação para os empregados designados e compra de software que auxilie na análise de cenários
Quanto? (How Much)	Entre R\$ 5.000,00 e R\$ 10.000,00.

Fonte: Dados da pesquisa, 2023

### Plano 3: Melhoria nos sistemas, dados e modelos de informação

Para que seja alcançado o terceiro objetivo, os gestores da Cagece deverão implementar o software adquirido por meio de licitação que tem como objetivo principal facilitar o processo de gestão de riscos. Para validar esse investimento será necessário fazer com que o sistema sirva às principais demandas que serão ordenadas pela GRC. O Quadro 14 a seguir apresenta a proposta elaborada.

QUADRO 14 – PLANO DE AÇÃO 3

Implementar software de gestão de riscos em toda a Companhia	
5W	
O quê? (What)	Implementar sistema de informação adquirido por meio de licitação



Por quê? (Why)	O software agirá como facilitador às tarefas do processo de gestão de riscos, fazendo com que haja menos erros
Onde? (Where)	Em todos os níveis hierárquicos da Companhia
Quem? (Who)	Gerência de Governança, Riscos e Conformidade
Quando? (When)	Em até 6 meses após a implementação efetiva na GRC
<b>2H</b>	
Como? (How)	Por meio de treinamentos internos com a equipe que já domina sua execução
Quanto? (How Much)	-

Fonte: Dados da pesquisa, 2023

#### Plano 4: Cultura de gerenciamento de riscos, comunicação e treinamento e monitoramento e melhoria contínua

Apesar de a Cagece estar constantemente motivada a disseminar a cultura de gestão de riscos, inclusive contando com um Programa de Disseminação voltado para este objetivo, ainda é possível identificar algumas lacunas que podem dificultar o gerenciamento dos riscos. Como exemplo pode-se citar quando um gestor de área prioriza outra tarefa em detrimento de gerenciar seus riscos e faz sua ordem de prioridades, fazendo com que seus superiores precisem cobrar para que aquela obrigação seja concluída.

Nesse aspecto é interessante que a gestão identifique essas áreas mais resistentes e promova o estímulo à execução destas práticas, explicando a importância da gestão de riscos para a empresa. A proposta é que além dos treinamentos já existentes e do fórum anual, seja possível uma conversa mais próxima da GRC com os Grupos de Trabalho em que sejam discutidas as ações realizadas em cada área trabalhada em forma de mesa redonda ou palestras rápidas. O Quadro 15 a seguir apresenta a proposta elaborada.

#### QUADRO 15 – PLANO DE AÇÃO 4

Promoção de ações integrativas	
<b>5W</b>	
O quê? (What)	Promover ações que integrem os grupos de trabalho de cada área com conversas, mesas redondas ou palestras que valorizem a gestão de riscos

Por quê? (Why)	As áreas mais resistentes precisam conviver e perceber a importância da gestão de riscos em suas atividades rotineiras
Onde? (Where)	Em cada área que apresente resistência identificada pela GRC
Quem? (Who)	Gerência de Governança, Riscos e Conformidade
Quando? (When)	Anualmente
<b>2H</b>	
Como? (How)	Por meio de conversas, mesas redondas e palestras
Quanto? (How Much)	-

Fonte: Dados da pesquisa, 2023

### **Responsáveis pelo relatório técnico**

Marília Gabrielly Dantas de Moraes

Mestranda do Programa de Mestrado Profissional em Administração Pública

UFERSA Mossoró

marilliagabrielly@uern.br

Álvaro Fabiano Pereira de Macedo

Doutor em Administração pela PUC-PR

UFERSA Mossoró

alvarofabiano@ufersa.edu.br