1. OBJETIVO

O objetivo desta Política é estabelecer as diretrizes para a gestão integrada de riscos corporativos no âmbito da Compagas.

2. ABRANGÊNCIA

Esta Política aplica-se a toda Compagas.

3. DEFINIÇÕES

3.1 Apetite ao Risco - Os tipos e a exposição ao risco que a Compagas está disposta a aceitar ou a rejeitar na busca por criação de valor.

3.2 Comitê de Gestão de Riscos Corporativos - Órgão nomeado pela Diretoria Executiva, com composição multidisciplinar para tratar, sob demanda, questões relativas à gestão integrada de riscos corporativos, tendo como objetivo principal a identificação e avaliação dos riscos aos quais a Companhia está exposta, de forma a fortalecer a gestão dos recursos e a proteger e valorizar seu patrimônio.

3.3 Controle - Política ou Procedimento que é parte do Controle Interno. É desenhado para evitar um evento ou resultado indesejado.

3.4 Controle Interno - Processo conduzido pela estrutura de Governança, Administração e outros profissionais da organização, desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados à eficiência e eficácia das operações, confiabilidade dos reportes e conformidade com leis e regulamentos.

3.5 COSO ERM - *Enterprise Risk Management – framework "*Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance" publicado em 2017 pelo *Committee of Sponsoring Organizations of the Treadway Comission - COSO*.

3.6 Evento - Fato ou conjunto de acontecimentos que caracteriza a materialização do risco. No contexto de risco, os eventos vão além das transações rotineiras: incluem aspectos de negócios mais amplos, como mudanças na estrutura de governança e operacional, influências geopolíticas e sociais e negociações de contratos, entre outros.

3.7 Fator de Risco - Qualquer condição que, combinada ou individualmente, possa potencializar a probabilidade de materialização do risco. Causa de um evento.

3.8 Gerenciamento de Riscos Corporativos - Cultura, competências e práticas, integradas à definição de estratégia e sua execução, em que a organização se apoia para gerenciar os riscos na criação, preservação e realização de valor.

3.9 Impacto - Resultado ou efeito de um risco. Pode haver uma variedade de possíveis impactos associados a um risco, entre os quais: financeiro, operacional, imagem e socioambiental. O impacto de um risco pode ser positivo ou negativo em relação à estratégia ou aos objetivos de negócio da organização e graduado em muito alto, alto, médio, baixo e muito baixo.

3.10 Mapa de Calor (*heatmap*) - Representação gráfica para destacar a severidade (magnitude) relativa de cada um dos riscos que ameaçam a concretização de uma determinada estratégia ou objetivo de negócio.

3.11 Modelos das Três Linhas - O Modelo das Três Linhas, elaborado e divulgado pelo The IIA, *The Institute of Internal Auditors*, orienta as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos.

3.12 Nível de Risco - Consiste na relação entre a probabilidade e a avaliação final do impacto e poderá ser visualizado no mapa de calor (*heatmap*). A classificação do risco poderá ser:
- *Alto:* significante potencial de impacto negativo. Ações robustas e imediatas devem ser endereçadas pela Gestão.
- *Médio:* moderado potencial de impacto negativo. A gestão deve endereçar ações para redução da exposição dentro de prazo adequado.
- *Baixo:* baixo potencial de impacto negativo. Devem ser monitorados periodicamente pela Gestão.

3.13 Plano de Ação – Planejamento e acompanhamento das atividades necessárias para assegurar que as respostas aos riscos sejam realizadas com eficácia para atingimento do resultado desejado.

3.14 Probabilidade - Indica a possibilidade de ocorrência de um dado evento. Pode ser expressa em termos quantitativos, como: percentagem, frequência de ocorrência, ou outra métrica numérica, ou em termos qualitativos, como: muito alta, alta, média, baixa, muito baixa.

3.15 Processo de Gestão de Risco - Processo coordenado pela Gerência de Governança, Risco e *Compliance,* do qual também fazem parte o Comitê de Gestão de Riscos Corporativos, Gestores, Diretoria Executiva, Comitê de Auditoria Estatutário e o Conselho de Administração, visando levantar os principais riscos e impactos inerentes ao modelo de negócio da Compagas, proporcionando o aprimoramento dos processos de gestão e apoio à tomada de decisão.

3.16 Resposta aos Riscos - A decisão de aceitar, transferir, evitar ou mitigar o risco.

3.17 Risco - Possibilidade de que um evento venha a ocorrer e afete adversamente o alcance da estratégia e dos objetivos de negócio. O risco pode ser inerente, quando da ausência de ações de tratamento que visem a alterar a probabilidade ou o impacto da materialização do risco, e residual, tratando-se de risco remanescente, posterior a adoção de ações de tratamento do risco inerente.

4. CATEGORIAS DOS RISCOS

É a estrutura adotada pela Compagas para agrupar os riscos de acordo com as categorias de objetivos que consideram a natureza destes e sua relação com o apetite ao risco:

4.1 Risco Estratégico: relacionado ao atingimento dos objetivos estratégicos da Compagas, considerando fatores macroeconômicos, sociais, políticos, ambientais, entre outros, que possam (i) afetar direta ou indiretamente a imagem da Companhia, (ii) impactar sua missão, visão e valores, (iii) gerar perda substancial no valor econômico da Compagas.

4.2 Risco Financeiro: está associado à (i) possibilidade de emissão de relatórios financeiros, gerenciais, regulatórios, fiscais, estatutários e de sustentabilidade incompletos, inexatos ou intempestivos, expondo a Compagas a multas, penalidades ou outras sanções, ou afetando negativamente os interesses e as tomadas de decisões dos *stakeholders*; (ii) possibilidade de insuficiência de recursos, caixa ou outro ativo financeiro, para liquidar as obrigações nas datas previstas; (iii) possibilidade de perdas decorrentes da dificuldade de recebimento de valores faturados a seus clientes ou de uma contraparte em um instrumento financeiro, resultantes da falha destes em cumprir com suas obrigações contratuais; (iv) possibilidade de

que o valor justo ou os fluxos de caixa futuros de instrumento financeiro oscilem devido a mudanças nos preços de mercado, tais como as taxas de câmbio, taxas de juros e preços de ações.

4.3 Risco Operacional: relaciona-se à eficácia e à eficiência das operações da Compagas, inclusive as metas de desempenho financeiro e operacional e a salvaguarda de ativos e à possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos, como catástrofes naturais, greves e atos terroristas

4.4 Risco de Conformidade/*Compliance*: relaciona-se ao não cumprimento de legislação, políticas, normas e regulamentos internos e aqueles que regem o mercado de atuação da empresa, bem como os princípios de conduta ética, íntegra e socioambientais. Estão englobados nesta categoria os riscos relacionados à fraude e corrupção.

5. PREMISSAS

5.1 Definição, por parte da Alta Administração, do apetite ao risco que a Compagas está disposta a aceitar ou rejeitar na busca por criação de valor.

5.2 A integração das práticas de gerenciamento de riscos corporativos por toda a organização é capaz de otimizar a tomada de decisões sobre governança, estratégia, definição de objetivos e operações, desta forma, possibilitando a melhoria contínua dos resultados ao conectar mais estreitamente a estratégia e os objetivos do negócio ao risco ao qual a organização está sujeita. O esforço exigido para integrar o gerenciamento de riscos corporativos proporciona à Compagas maior percepção sobre suas forças e oportunidades, colaborando para construção de um caminho claro para criar, preservar e realizar valor.

5.3 As diretrizes desta política estão fundamentadas nos valores da Compagas, no seu Código de Ética e Integridade e nas orientações do COSO ERM.

5.4 A Compagas adota o modelo de Gestão de Riscos Corporativos baseado no modelo das Três Linhas, conforme apresentado abaixo:

- **Primeira linha**: gestão operacional, composta pelas Diretorias Executivas, gerentes, assessores das áreas de negócios e donos de controles. São as funções que gerenciam e têm propriedade sobre os riscos, responsáveis por implementar ações corretivas para resolver deficiências em processos e controles. Também tem a atribuição de identificar, avaliar, controlar e reduzir os riscos guiando o desenvolvimento e a implementação de políticas e procedimentos internos, garantindo que as atividades estejam de acordo com as metas e objetivos;
- **Segunda linha**: composta pela Gerência de Governança, Risco e *Compliance* - Responsável pelo apoio, monitoramento e supervisão no gerenciamento dos riscos, auxiliando no desenvolvimento e/ou monitoramento dos controles da primeira linha, apoiando as políticas de gestão, auxiliando no desenvolvimento de processos e controles, fornecendo orientações e treinamento, facilitando e monitorando a implementação de práticas eficazes de gerenciamento de riscos por parte da gestão operacional, monitorando a adequação e a eficiência do controle interno, a precisão e a integridade do reporte, a conformidade com leis e regulamentos e a resolução oportuna de deficiências;
- **Terceira linha:** Estrutura organizacional independente, composta pela Auditoria Interna, responsável por aferir a adequação do controle interno e a efetividade do gerenciamento de riscos, recomendando, quando necessário, melhorias nos processos.

6. DIRETRIZES

6.1 Manter a Política de Gestão Integrada de Riscos alinhada com a estratégia e os objetivos da Compagas.
6.2 Manter efetividade e conformidade no ambiente de Controle Interno.
6.3 Integrar o processo de Gestão de Riscos em todos os processos organizacionais e nas relações

comerciais com fornecedores e parceiros de negócio.
6.4 Adotar indicadores de desempenho empresarial para o monitoramento dos riscos.
6.5 Aprimorar constantemente o gerenciamento de riscos que envolvem os negócios da Compagas.
6.6 Considerar os aspectos relacionados à sustentabilidade, com ênfase às questões socioambientais e de saúde e segurança, buscando antecipar, avaliar e reduzir os impactos negativos de curto, médio e longo prazo das operações à sociedade.
6.7 Adotar critérios, integrar e manter os níveis de apetite ao risco alinhados com as dimensões de estratégia, negócios e finanças da Compagas, submetendo periodicamente à apreciação do Conselho de Administração.
6.8 Direcionar as oportunidades identificadas às áreas competentes para análise e implementação das ações necessárias à sua realização.
6.9 Promover a cultura da gestão de riscos, oferecer orientação e treinamento, elaborar e divulgar informações sobre riscos, cultura e performance abrangendo a Companhia como um todo.
6.10 Desenvolver uma visão de portfólio consolidado de riscos corporativos que melhore a capacidade da organização de articular o nível de risco assumido na busca da estratégia e dos objetivos de negócio.
6.11 Identificar riscos novos e emergentes de modo que a administração possa implementar respostas tempestivamente e avaliar periodicamente os riscos identificados.
6.12 Monitorar a adequação e eficácia das respostas aos riscos, a precisão e integridade das divulgações e a correção tempestiva das deficiências.
6.13 Maximizar a utilização dos sistemas de informação e tecnologias existentes na empresa para impulsionar o gerenciamento de riscos corporativos.
6.14 Submeter trimestralmente à análise do Comitê de Auditoria Estatutário e semestralmente à análise do Conselho de Administração o portfólio de riscos e os planos de mitigação decorrentes.

7. RESPONSABILIDADES

7.1 CONSELHO DE ADMINISTRAÇÃO – CAD

- Aprovar a Política de Gestão Integrada de Riscos Corporativos;
- Avaliar e aprovar o alinhamento do apetite ao risco aos processos de Gestão Estratégica;
- Acompanhar a efetividade do processo de Gestão de Riscos na Compagas;
- Analisar trimestralmente o portfólio de riscos e os planos de mitigação decorrentes;
- Implementar e supervisionar os sistemas de Gestão de Riscos e de Controle Interno estabelecidos para a prevenção e a mitigação dos principais riscos aos quais a Companhia está exposta, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude.

7.2 COMITÊ DE AUDITORIA ESTATUTÁRIO – CAE

- Avaliar a efetividade do processo de Gestão de Riscos na Compagas;
- Revisar a Política de Gestão Integrada de Riscos Corporativos;
- Analisar trimestralmente o portfólio de riscos e os planos de mitigação decorrentes.

7.3 DIRETORIA EXECUTIVA

- Patrocinar a implantação da Gestão de Riscos no âmbito de sua atuação;
- Apoiar os gestores de riscos no estabelecimento das ações de tratamento e dos mecanismos de controles para os riscos e incidentes identificados;
- Apoiar a Gerência de Governança, Risco e *Compliance* na elaboração do portfólio de riscos corporativos;
- Acompanhar a efetividade do processo de Gestão de Riscos na Compagas;
- Analisar semestralmente o portfólio de riscos e os planos de mitigação decorrentes.

7.4 GESTORES

- Identificar os riscos, as suas causas e o seus impactos para a Compagas;
- Estabelecer as ações de tratamento e os mecanismos de controles adequados para cada risco;

- Realizar o monitoramento periódico dos riscos sob sua responsabilidade;
- Reportar à Diretoria da área envolvida e à Gerência de Governança, Risco e *Compliance* os riscos altos e críticos, para análise e avaliação, de acordo com a Metodologia de Gestão de Riscos e os padrões definidos; bem como os eventos de materialização dos riscos.

7.5 GERÊNCIA DE GOVERNANÇA, RISCO E *COMPLIANCE*

- Definir e coordenar a implantação das diretrizes, políticas, metodologias e práticas de gerenciamento de riscos corporativos na Compagas;
- Promover treinamentos e acompanhar a aplicação das etapas de identificação do risco, avaliação da severidade, priorização do risco e a implementação de respostas aos riscos;
- Disseminar e monitorar a adequada aplicação das políticas e metodologias;
- Coordenar as atividades do Comitê de Gestão de Riscos Corporativos;
- Elaborar, acompanhar e administrar o portfólio de Riscos Corporativos da Compagas;
- Monitorar as ações de tratamento e os mecanismos de controles para os riscos identificados;
- Apresentar o Portfólio de Riscos Corporativos periodicamente ao Conselho Fiscal, ao Comitê de Auditoria Estatutário, a Diretoria Executiva e ao Conselho de Administração;
- Reportar, periodicamente, as atividades de Gestão de Riscos ao Comitê de Auditoria Estatutário e ao Conselho de Administração;
- Promover e incentivar a conscientização sobre riscos em toda a Companhia.

7.6 COMITÊ DE GESTÃO DE RISCOS CORPORATIVOS

- Identificar e avaliar os riscos corporativos, classificando-os e avaliando-os quanto ao impacto e probabilidade, de acordo com a presente política e demais normativos internos que disciplinam a matéria;
- Emitir recomendações para o tratamento dos riscos identificados;
- Monitorar os planos de ação propostos para a mitigação dos riscos identificados.

7.6 AUDITORIA INTERNA

- Avaliar a efetividade do processo de Gestão de Riscos na Compagas;
- Avaliar a adequação das ações de tratamento e mecanismos de Controles Internos, recomendando, quando necessário, melhorias nos processos ao gestor de riscos;
- Realizar reportes periódicos de suas avaliações ao Comitê de Auditoria Estatutário e ao Conselho de Administração;

8. REFERÊNCIAS

- Lei nº 12.846/2013 (Lei Anticorrupção);
- Decreto Federal nº 8.420/2015 (Regulamenta a Lei Anticorrupção);
- Lei nº 13.303/2016 (Lei das Estatais);
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD)
- COSO – ERM*: Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management* (2017);
- Política de Governança Corporativa;
- Política de Sustentabilidade;
- Política de Integridade;
- Política de Segurança da Informação;
- Política de Privacidade e Proteção de Dados Pessoais.

9. SUBSTITUIÇÃO DE VERSÃO

Esta versão substitui a Revisão 00, de 20/06/2018.

10. APROVAÇÃO E VIGÊNCIA

Esta Política foi aprovada na 221ª Reunião do Conselho de Administração, de 27/06/2022, com vigência a partir desta data.