

POLÍTICA DE GERENCIAMENTO DE RISCOS DA COMERC PARTICIPAÇÕES S.A.

1. OBJETIVO

- 1.1. A presente Política de Gerenciamento de Riscos (“Política”), aprovada na reunião do Conselho de Administração da Comerc Participações S.A. (“Companhia”) realizada em 6 de agosto de 2021, visa estabelecer e divulgar princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos na Companhia, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos inerentes às atividades da Companhia e que possam afetar o atendimento aos seus objetivos e realização de seus negócios.

2. REFERÊNCIAS

- 2.1. Esta Política tem como referência:

- (i) as diretrizes de governança corporativa do estatuto social da Companhia;
- (ii) as normas aplicáveis emanadas pela Comissão de Valores Mobiliários (CVM);
- (iii) as diretrizes e princípios descritos no Código de Ética e Conduta Empresarial da Companhia;
- (iv) *benchmarking* do mercado, principalmente com relação ao setor de energia;
- (v) o relatório de diagnóstico dos riscos aos quais a Companhia está exposta, elaborado por assessores externos em maio de 2021; e
- (vi) o modelo do COSO-ERM - *Committee of Sponsoring Organizations of Treadway Commission* (“COSO-ERM”).

3. ABRANGÊNCIA

- 3.1. Esta Política é aplicável à todas as áreas da Companhia e de suas controladas.

4. DEFINIÇÕES

- 4.1. Auditoria Interna: área responsável pela auditoria interna da Companhia, nos termos previstos nesta Política.
- 4.2. Categorias de Riscos: os Riscos são classificados em 8 (oito) categorias: (i) estratégicos (que dentre outros engloba o risco político); (ii) operacionais; (iii) financeiros; (iv) tecnológicos; (v) socioambientais; (vi) legais; (vii) reputacionais; e (viii) de mercado, os quais, de forma conjunta, representam os Riscos da Companhia.
- 4.3. Comitê de Auditoria: o Comitê de Auditoria da Comerc Participações S.A., órgão de assessoramento vinculado ao Conselho de Administração.
- 4.4. Comissão de Ética e Compliance: grupo de trabalho da Comerc Participações S.A., destinado a auxiliar a Área de Compliance, Riscos Corporativos e Controles Internos na coordenação de melhorias de processos para mitigar os Riscos Legais e Reputacionais.
- 4.5. Conselho de Administração: o Conselho de Administração da Comerc Participações S.A.
- 4.6. Diretoria: o corpo de diretores da Comerc Participações S.A.

- 4.7. Área de Compliance, Riscos Corporativos e Controles Internos: área responsável pelo desempenho das funções de controles internos, gerenciamento de Riscos e *Compliance* da Companhia, nos termos previstos nesta Política.
- 4.8. Matriz de Riscos: visa estabelecer uma comparação individual dos Riscos a partir dos impactos e probabilidades de ocorrência para fins de priorização e gestão. A matriz de riscos é um documento em constante evolução e que deve ser atualizada, no mínimo, anualmente, por ocasião da revisão de planejamento estratégico da Companhia e, tempestivamente, com o surgimento de eventos de Risco emergentes.
- 4.9. Limite (ou Appetite) de Riscos: é a exposição e/ou impacto máximo do Risco que a Companhia está disposta a aceitar, na busca dos objetivos e geração de valor. Nem todos os tipos de Riscos são passíveis de aceitação. Portanto, a proposta de limites deverá obrigatoriamente ser fundamentada e formalizada pelas seguintes análises: (i) avaliação do retorno tangível e intangível relacionado ao limite de Risco proposto; (ii) capacidade da Companhia de suportar o impacto do limite de Risco proposto (iii) decisão se o Risco deve ou não ser aceito conforme sua tipologia; (iv) viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e (v) disponibilidade de recursos (investimento e esforço) para implantação.
- 4.10. Proprietário do Risco: colaboradores integrantes das áreas de negócios da Companhia, que possuem o maior domínio e conhecimento técnico acerca do Risco correspondente, responsável pela tomada de decisão e capaz de estabelecer e gerir os planos de ação para adequar a exposição aos limites aprovados.
- 4.11. Risco(s): todo e qualquer evento decorrente de incertezas que a Companhia está exposta e que possa impactar negativamente o alcance dos objetivos e de geração de valor estabelecidos no seu plano estratégico de longo prazo.

5. RISCOS AOS QUAIS A COMPANHIA ESTÁ EXPOSTA

- 5.1. As principais Categorias de Riscos aos quais a Companhia busca proteção estão elencadas a seguir:

5.2. Riscos Estratégicos

São aqueles associados à estratégia da Companhia na busca de criação, proteção e crescimento de valor e incluem os riscos concorrenciais, riscos políticos e riscos de imagem/reputacionais. São causados por mudanças no ambiente externo, tais como político e econômico, mercado, competidores, fusões e aquisições, disponibilidade de recursos, inovações e portfólio de produtos e/ou serviços.

5.3. Riscos Operacionais

São aqueles que envolvem a operação, sistemas, processos, controles internos, clientes, receitas e outros ativos da Companhia que podem implicar perdas financeiras, danos de reputação e imagem, declínio dos resultados da Companhia. Dentre eles, podemos citar: inviabilidade dos serviços ou soluções oferecidos pela Companhia, incremento de custos de operação ou equipamentos, indisponibilidade dos equipamentos de geração de energia, inadimplementos contratuais de clientes ou parceiros, ausência de prestadores de serviços ou de mão de obra interna especializada, dentre outros.

5.4. Riscos Financeiros

São aqueles decorrentes de efeitos não esperados no cenário econômico, político e nas tendências de mercado que podem ter reflexo no comportamento do consumidor, na taxa de

juros, inflação, investimentos financeiros, dentre outros. Dentre eles, podemos citar: perda financeira devido a aplicações financeiras equivocadas, perdas financeiras decorrentes de ações ocasionadas por distratos realizados pelos clientes, perda financeira por variação cambial ou de juros, riscos de refinanciamento de dívidas, dentre outros.

5.5. Riscos Tecnológicos

São aqueles que podem ser causados pelo vazamento de dados/informações pessoais, roubo/vazamento de informações estratégicas (envio de arquivos confidenciais), tratamento inadequado ou irregular de dados pessoais, acesso inadequado a ativos e recursos de TI, acesso remoto inseguro, interrupções na rede de transmissão ou no processamento de dados, interrupção no funcionamento dos sistemas de monitoramento e controle dos ativos de geração e demais negócios da Companhia, dentre outros, que impactam na confidencialidade, integridade e disponibilidade das informações.

5.6. Riscos Socioambientais

São os riscos relacionados a questões ambientais, como a contaminação de água e solo, descarte indevido de resíduos de construção, e corte indevido de árvores nativas, e questões socioambientais, como riscos de perdas decorrentes de efeitos negativos das atividades e operações da Companhia sobre a sociedade.

5.7. Riscos Legais

São os riscos relacionados a eventuais descumprimentos ou potenciais descumprimentos das legislações vigentes no ordenamento jurídico brasileiro e determinações feitas pelos órgãos reguladores do setor elétrico, as quais a Companhia está submetida e que podem gerar danos ou perdas aos negócios da Companhia. Dentre eles, podemos citar: atividades executadas em desacordo com políticas, normas e procedimentos da Companhia, falhas no monitoramento de alteração/criação de leis e regulamentações, sanções/multas devido à transmissão de informações incorretas para órgãos regulatórios, fraude por substituição ou inclusão de pagamentos e/ou despesas pessoais, dentre outros.

5.8. Riscos Reputacionais

São os riscos que impactam diretamente na imagem, reputação e percepção da Companhia perante o mercado, seus colaboradores, comunidades onde estão localizados os ativos de geração, parceiros comerciais e fornecedores. Os Riscos Reputacionais podem decorrer dos Riscos Legais, Operacionais, Socioambientais, entre outros.

5.9. Riscos de Mercado

São os riscos relacionados a potencial perdas que podem decorrer das variações nos preços de energia, os quais podem comprometer o valor das operações de trading da Companhia para compra e venda de energia.

6. DIRETRIZES

6.1. Na condução dos negócios, a Companhia assume Riscos que, se não identificados e tratados de forma adequada, podem comprometer seus valores, reputação, competitividade e perenidade dos negócios.

6.2. Toda e qualquer decisão envolve determinado grau de Risco. Deve-se destacar que os Riscos jamais serão eliminados. O objetivo é entendê-los, avaliar e definir ações de resposta para que as perdas sejam reduzidas e previstas.

6.3. A análise de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis. Para

todos os efeitos, os Riscos com limites aprovados devem ser levados em consideração na elaboração de projeções, adequando as metas se necessário, aos limites de riscos aprovados.

- 6.4. É fundamental o entendimento e disseminação entre os órgãos e executivos envolvidos, da correta diferenciação de impactos causados por eventos e situações como: (i) falhas de controles internos em processos; (ii) decisões estratégicas malsucedidas; ou (iii) falha na governança. Este entendimento visa aperfeiçoar e fortalecer o modelo de governança corporativa da Companhia.
- 6.5. Todos os Riscos desenvolvidos, com limites aprovados, deverão ser formalizados em relatórios detalhados, explicativos, com planos de ação, se for o caso, detalhados com responsáveis e prazos de conclusão. Os relatórios deverão ser assinados pelo Proprietário do Risco e pelo Comitê de Auditoria.

7. METODOLOGIA

- 7.1. A Companhia identifica, avalia, trata e monitora todos os Riscos a que está exposta de forma a garantir o cumprimento das metas estabelecidas em seu planejamento estratégico.
- 7.2. O processo de gerenciamento de Riscos da Companhia é baseado (mas não se limita), no COSO-ERM e é composto pelas seguintes etapas:
- A.** *Identificação dos riscos:* identificação dos fatores (causas) de Riscos e implicações nos objetivos (metas e resultados) projetados, através da utilização dos seguintes instrumentos: (i) entrevistas com pessoas-chave da Companhia; (ii) auditorias nos processos internos; e (iii) análise de denúncias enviadas por meio do Canal Aberto, disciplinado no Código de Ética e Conduta Empresarial.
- B.** *Avaliação:* cálculo do impacto e probabilidade de ocorrência dos Riscos sobre os resultados projetados. Os seguintes critérios são utilizados:

Eixo da Probabilidade

Probabilidade	Peso
Quase certo: é praticamente impossível evitar que o risco identificado aconteça.	5
Alta: a chance do risco ocorrer é grande e frequentemente ele ocorre de fato.	4
Média: probabilidade ocasional de acontecimento do risco.	3
Baixa: pouca chance de acontecer algum problema advindo desse risco.	2
Rara: é bastante improvável que o risco aconteça.	1

Eixo do Impacto

Impacto	Peso
Gravíssimo: alto impacto, podendo causar dano irreversível à empresa.	5
Grave: compromete de forma acentuada o resultado ou a empresa.	4
Médio: perda momentânea que pode ser corrigida, mas com impactos.	3
Leve: desvio quase imperceptível e que pode ser facilmente corrigido	2
Sem Impacto: não gera nenhum tipo de problema perceptível.	1

- C.** Limite de Risco: priorização e definição do Limite de cada Risco que a Companhia está disposta a correr na busca pelo retorno e geração de valor, classificando os Riscos como de acordo com as definições abaixo:
- (i) *Risco Gravíssimo:* representam ameaça potencial aos negócios da Companhia, podendo causar danos irreversíveis. Demandam ação gerencial prioritária para eliminar o componente de Risco ou ao menos reduzir sua severidade e/ou frequência.
 - (ii) *Risco Grave:* com alto impacto e baixa frequência e compromete de forma acentuada os negócios da Companhia. Devem ser quantificados e monitorados regularmente para direcionar continuamente as estratégias de mitigação e/ou planos de contingência. O objetivo é estar preparado caso o evento venha a acontecer. Tratamento sujeito à viabilidade de contratação de seguros como resposta a estes Riscos.
 - (iii) *Risco Médio:* de menor criticidade devido ao menor nível de impacto no valor dos negócios, gera uma perda momentânea que pode ser corrigida. O foco deve ser o de definir níveis aceitáveis de perda por eventos e limites de competência que evitem que o nível de impacto suba ao longo do tempo.
 - (iv) *Risco Leve:* perdas de menor relevância, podendo o custo do impacto ser menor do que o custo de mitigá-los. Riscos de baixo impacto e frequência, não havendo necessidade de monitoramento contínuo.
 - (v) *Risco Sem Impacto:* riscos imperceptíveis que não geram nenhum dano potencial à Companhia, não havendo necessidade de monitoramento contínuo.
- D.** Tratamento: a partir da identificação e avaliação dos Riscos, são implementadas respostas, que consistem no tratamento e mitigação dos Riscos. As respostas aos Riscos consideram os seguintes critérios:
- (i) *Eliminar:* eliminar totalmente a fonte do Risco. Esta resposta é aplicável na situação em que Companhia não encontrou alternativas para mitigação do Risco até um nível aceitável, em conformidade com seu Limite de Riscos;
 - (ii) *Transferir e/ou Compartilhar:* transferir a responsabilidade do Risco para terceiros por meio de terceirização de operações e atividades;
 - (iii) *Mitigar:* reduzir a probabilidade e/ou impacto de um Risco para um limite aceitável para a Companhia;
 - (iv) *Aceitar/Reater:* nenhuma ação direta é tomada para alterar o nível de impacto ou probabilidade do Risco. Esta resposta é aplicável quando o Risco está abrangido no Limite de Riscos da Companhia.
- E.** Planos de Ação: conjunto de iniciativas definidas e implantadas pelo Proprietário do Risco a fim de adequar as exposições aos limites aprovados (objeto de acompanhamento periódico).
- F.** Monitoramento: acompanhamento contínuo da adequação e da eficácia dos controles, assegurando que modelo de gerenciamento de Riscos está aderente aos objetivos da

Companhia ao longo do tempo.

8. RESPONSABILIDADES

8.1. Esta Política define e comunica os papéis e responsabilidades dos principais agentes envolvidos no processo de gestão de Riscos, desenhadas buscando-se a construção e implantação de um modelo que capture as experiências, percepções e os melhores conjuntos de informações disponíveis para a tomada de decisão.

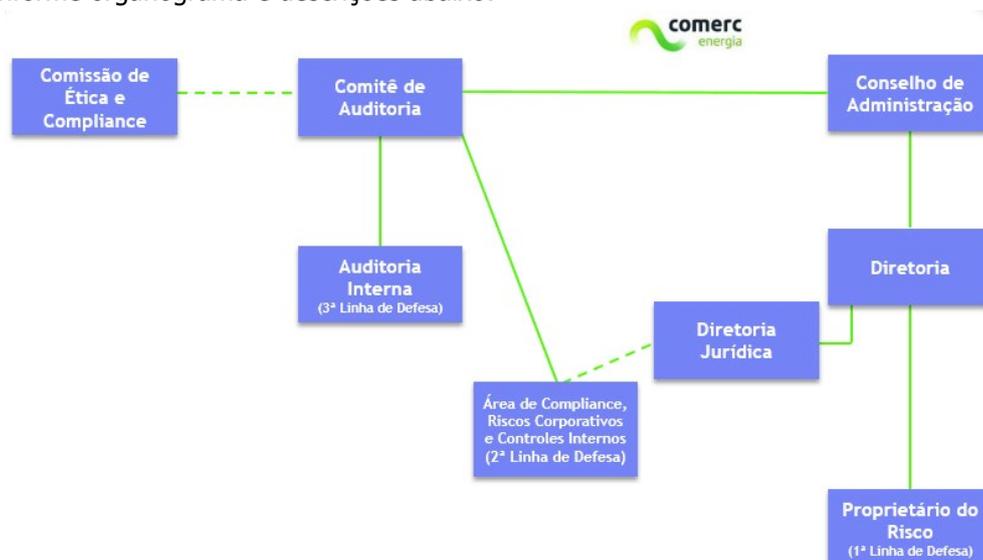
8.2. A estrutura de gerenciamento de Riscos da Companhia considera a atuação conjunta dos órgãos de governança corporativa e de gestão, e é realizada de acordo com o modelo de linhas de defesa do COSO-ERM. As linhas de defesa consistem em um conceito que define os papéis e responsabilidades no gerenciamento de riscos e fortalecimento da governança, bem como a interação desses papéis em todos os níveis da Companhia, conforme indicado abaixo:

A. 1ª Linha de Defesa: é representada pelos Proprietários de Riscos, responsáveis diretos pela execução de seus processos e detecção dos Riscos respectivos e implementação das respostas.

B. 2ª Linha de Defesa: é representada pela Área de Compliance, Riscos corporativos e Controles Internos, que atua em colaboração com a primeira linha, por meio do mapeamento e acompanhamento dos riscos e planos de ação a eles associados. A Área de Compliance, Riscos Corporativos e Controles Internos se reporta diretamente ao Comitê de Auditoria, e pode contar com o auxílio de outras áreas da Companhia, tais como controladoria e Auditoria Interna, para o desempenho de suas atividades. Os membros da Área de Compliance, Riscos Corporativos e Controles Internos não acumulam funções com atividades operacionais ou possuem relação de subordinação com áreas operacionais da Companhia. A Área de Compliance, Riscos Corporativos e Controles Internos reporta questões meramente administrativas à Diretoria Jurídica da Companhia, sem relação de subordinação.

C. 3ª Linha de Defesa: é representada pela área de Auditoria Interna, que atua no fornecimento de avaliações independentes à administração, especialmente pela realização de testes substantivos de controles internos para identificação de desvios operacionais e financeiros decorrentes de falhas e/ou fraudes.

8.3. Neste sentido, o processo de gerenciamento de Riscos da Companhia está estruturado conforme organograma e descrições abaixo:



8.4. Nesse contexto, compete ao **Conselho de Administração** da Companhia:

- (i) definir os objetivos estratégicos, adequado e aderente aos seus negócios e ao seu perfil de Riscos;
- (ii) aprovar as políticas e diretrizes de Risco;
- (iii) monitorar, anualmente, o mapa de exposição a Riscos a que a Companhia está exposta e influenciar na priorização dos Riscos a serem tratados;
- (iv) avaliar em pauta prévia, mudanças ou atualizações em cada Risco, cujos limites já tenham sido aprovados;
- (v) assegurar, ao Comitê de Auditoria, autonomia operacional, aprovando-lhe orçamento próprio destinado a cobrir despesas com seu funcionamento; e
- (vi) receber, por meio do Comitê de Auditoria, o reporte das atividades da área de Auditoria Interna, avaliando, ao menos anualmente, se a estrutura e orçamento desta são suficientes ao desempenho de suas funções.

8.5. Compete ao **Comitê de Auditoria** da Companhia, órgão autônomo de assessoramento vinculado ao Conselho de Administração, além do disposto em seu regimento interno:

- (i) acompanhar as atividades de identificação e avaliação dos Riscos aos quais a Companhia está exposta, e o desenvolvimento de ações que promovam redução de riscos e ameaças pela a serem elaborados pela Área de Compliance, Riscos Corporativos e Controles Internos;
- (ii) Recomendar ao Conselho de Administração da Companhia a avaliação de políticas, limites e planos de ação;
- (iii) avaliar, monitorar, e recomendar à administração a correção ou aprimoramento das políticas internas da companhia, incluindo a *Política de Transações com Partes Relacionadas e Demais Situações Envolvendo Conflito de Interesse*;
- (iv) monitorar o cumprimento desta Política e avaliar a performance frente aos limites de Risco aprovados;
- (v) opinar na contratação e destituição dos serviços de auditoria independente;
- (vi) avaliar a efetividade do modelo de gestão de Riscos e sugerir aprimoramentos no processo, apontando as causas e responsabilidades; e
- (vii) acompanhar as atividades da área de Auditoria Interna e da Área de Compliance, Riscos Corporativos e Controles Internos da Companhia e reportá-las ao Conselho de Administração.

8.6. Compete à **Diretoria** da Companhia:

- (i) atualizar a Matriz de Riscos sempre que ocorrer a revisão do plano estratégico e tempestivamente com o surgimento de fatores de risco emergentes;
- (ii) estabelecer priorização dos Riscos a partir do impacto e probabilidade, visando estabelecer uma comparação individual dos riscos para fins de priorização e gestão;
- (iii) avaliar e tomar decisões em relação a exposição aos Riscos (impacto e probabilidade) e aos limites apresentados pelos Proprietários dos Riscos e recomendar ações de respostas;

- (iv) acompanhar a evolução da exposição aos Riscos considerando os limites aprovados pelo Conselho de Administração;
 - (v) adotar Riscos avaliados como ferramenta de orientação da revisão ou construção do plano estratégico; e
 - (vi) disseminar a cultura da gestão de Risco em toda Companhia.
- 8.7. Compete à área de ***Auditoria Interna***, cujas atividades são reportadas ao Conselho de Administração por intermédio do Comitê de Auditoria, e que deverá ter estrutura e orçamento suficientes ao desempenho de suas funções:
- (i) aferir a qualidade e a efetividade do processo de gerenciamento de Riscos e dos processos de governança, da adequação dos controles e do cumprimento das normas e regulamentos associados aos negócios da Companhia, de forma independente, imparcial e tempestiva; e
 - (ii) fornecer relatórios anuais ao Comitê de Auditoria, a fim de garantir que o processo e estrutura de gerenciamento de Riscos (incluindo a Área de Compliance, Riscos Corporativos e Controles Internos) esteja sendo devidamente cumprida.
- 8.8. Compete à ***Área de Compliance, Riscos Corporativos e Controles Internos***, que possui reporte direto ao Comitê de Auditoria, é responsável pelas funções de compliance, riscos corporativos e controles internos na Companhia, e cujos membros não acumulam funções ou possuem relação de subordinação com áreas operacionais da Companhia:
- (i) fornecer apoio às áreas de negócios sobre o processo de gerenciamento de Riscos;
 - (ii) identificar e avaliar os Riscos aos quais a Companhia está exposta, para desenvolvimento de ações que promovam redução de riscos e ameaças;
 - (iii) acompanhar a execução e implementação dos planos de ação decorrentes dos trabalhos de controles internos na Companhia;
 - (iv) acompanhar e sugerir melhorias de controles internos nas áreas operacionais;
 - (v) zelar pelas atualizações, comunicação e aplicação do Código de Ética e Conduta Empresarial da Companhia; e
 - (vi) elaborar o plano de implantação dos procedimentos e diretrizes do Código de Ética Conduta Empresarial, bem como das demais políticas de integridade.
- 8.9. Compete à ***Comissão de Ética e Compliance***, grupo de trabalho que reporta trimestralmente ao Comitê de Auditoria:
- (i) auxiliar a Área de Compliance, Riscos Corporativos e Controles Internos na identificação e monitoramento dos Riscos e planos de ação para sua eliminação, mitigação ou controle
 - (ii) apurar comunicações recebidas através do Canal Aberto, com o auxílio da Área de Compliance, Riscos Corporativos e Controles Internos;
 - (iii) propor as medidas disciplinares aplicáveis em casos de violação ao Código de Ética e Conduta e/ou à legislação;
 - (iv) monitorar a aplicação do Código de Ética e Conduta;

- (v) deliberar acerca da contratação de investigação independente, quando necessário; e
- (vi) analisar e acompanhar informações de potenciais situações de conflito de interesses informadas pelos colaboradores por meio do Formulário de Conflito de Interesses.

8.10. Compete aos ***Proprietários dos Riscos*** da Companhia:

- (i) identificar os fatores de Riscos e indicadores para a mensuração e monitoramento dos Riscos;
- (ii) fornecer informações precisas, íntegras e suficientes para análise;
- (iii) apresentar percepção quanto à exposição ao Risco, se possível, pautada também em indicadores de mercado;
- (iv) sugerir, avaliar, implantar e monitorar as ações com o objetivo de reduzir a exposição ao Risco sob sua responsabilidade;
- (v) comunicar, tempestivamente, os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas; e
- (vi) dar cumprimento ao plano de ação.

8.11. Compete à ***Comissão de Riscos***, grupo de trabalho independente vinculado ao Conselho de Administração, acompanhar os riscos de mercado, especialmente aqueles relacionados as operações de trading da Companhia, além de recomendar eventuais operações e contratos para deliberação do Conselho de Administração.

9. DISPOSIÇÕES GERAIS

- 9.1. No caso de conflito entre as disposições desta Política e do Estatuto Social, prevalecerá o disposto no Estatuto Social, e em caso de conflito entre as disposições desta Política e da legislação vigente, prevalecerá o disposto na legislação vigente.
- 9.2. Caso qualquer disposição desta Política venha a ser considerada inválida, ilegal ou ineficaz, essa disposição será limitada, na medida do possível, para que a validade, legalidade e eficácia das disposições remanescentes desta Política não sejam afetadas ou prejudicadas.
- 9.3. As violações dos termos da presente Política serão examinadas pelo Conselho de Administração, que adotará as medidas cabíveis, alertando, ainda, que certas condutas poderão constituir infração à legislação aplicável, sujeitando os responsáveis às penas previstas na legislação vigente.
- 9.4. Esta Política entra em vigor na data de sua aprovação e somente poderá ser modificada por deliberação do Conselho de Administração da Companhia e pode ser consultada em <http://www.comerc.com.br/ri>.

* * *