POLÍTICA DE GERENCIAMENTO DE RISCOS



méliuz

méliuz

SUMÁRIO

CAPÍTULO I - DEFINIÇÕES	3
CAPÍTULO II - OBJETIVO E APLICAÇÃO	4
CAPÍTULO III - DIRETRIZES E PROCESSOS DE GERENCIAMENTO DE RISCOS	4
CAPÍTULO IV - CATEGORIAS DE RISCOS	6
CAPÍTULO V - RESPONSABILIDADES E COMPETÊNCIAS	7
CAPÍTULO VI - VIGÊNCIA	10
CAPÍTULO VII - DISPOSIÇÕES GERAIS	10
Anexo I	12

CAPÍTULO I - DEFINIÇÕES

1.1. Quando não definidos em outros dispositivos desta Política, os termos iniciados em letra maiúscula, estejam no singular ou no plural, no masculino ou no feminino, terão os seguintes significados:

- **"Administradores"** significa, exclusivamente, os membros do Conselho de Administração e os Diretores estatutários da Companhia, nos termos da Lei das Sociedades por Ações e do Estatuto Social.
- **"Auditoria Interna"** significa a função independente de auditoria interna da Companhia, própria ou exercida por auditor independente contratado para essa finalidade, a depender do escopo da auditoria, com reporte funcional ao Conselho de Administração, diretamente ou por meio do Comitê de Auditoria.
- **"Colaboradores"** significa os empregados, diretores não estatutários, aprendizes, estagiários e trabalhadores temporários da Companhia e de suas Controladas.
- **"Comitê de Auditoria"** significa o comitê de assessoramento vinculado ao Conselho de Administração, constituído e regido nos termos do Regulamento do Novo Mercado e de seu regimento interno.
- **"Comitês de Assessoramento"** significa os comitês estatutários ou não estatutários constituídos para assessorar o Conselho de Administração ou outros órgãos da Companhia, nos limites de seus regimentos e da legislação aplicável.
- **"Companhia"** significa o Méliuz S.A.
- **"Controladas"** significa as sociedades direta ou indiretamente controladas pela Companhia, conforme a legislação e as normas contábeis aplicáveis.
- **"COSO"** significa o Comitê de Organizações Patrocinadoras da Comissão Treadway (*Committee of Sponsoring Organizations of the Treadway Commission*), uma organização privada dedicada a fornecer orientações e diretrizes sobre gerenciamento de riscos corporativos, controles internos e prevenção de fraudes.
- **"Diretoria"** significa a Diretoria estatutária da Companhia, conforme previsto no Estatuto Social.
- **"Gerenciamento de Riscos"** significa o conjunto de atividades coordenadas, integradas à gestão da Companhia, para identificar, avaliar, tratar e monitorar os Riscos que possam afetar seus objetivos.
- **"Impacto"** significa a magnitude das consequências de um Risco sobre os objetivos da Companhia.
- **"Matriz de Riscos"** significa a ferramenta que representa graficamente os níveis de Risco resultantes da combinação entre Probabilidade e Impacto, consideradas a avaliação inerente, a efetividade dos controles e a avaliação residual.
- **"Pessoas Abrangidas"** significa os Administradores, os membros de Comitês de Assessoramento, os membros efetivos do Conselho Fiscal e seus suplentes quando em exercício ou com acesso à matéria, os Colaboradores e os terceiros que atuem em nome, benefício ou interesse da Companhia ou de suas Controladas, na extensão aplicável.
- **"Plano de Ação"** significa o conjunto documentado de medidas, responsáveis e prazos destinado a tratar um Risco ou uma deficiência de controle.
- **"Probabilidade"** significa a possibilidade de ocorrência de um Risco, avaliada segundo critérios qualitativos e, quando viável, quantitativos.
- **"Política"** significa esta Política de Gerenciamento de Riscos do Méliuz S.A.
- **"Proprietário do Risco"** significa o gestor designado com autoridade e responsabilidade pela gestão de determinado Risco, inclusive pela implementação e acompanhamento dos controles e Planos de Ação.
- **"Risco"** significa o efeito da incerteza sobre os objetivos da Companhia, que pode produzir impactos negativos ou positivos.
- **"Risco Inerente"** significa o nível de Risco antes da consideração dos controles existentes.
- **"Risco Residual"** significa o nível de Risco remanescente após a consideração do desenho e da efetividade dos controles e das demais respostas implementadas.
- **"Termo de Adesão"** significa o termo de ciência e compromisso previsto no Anexo I desta Política.

CAPÍTULO II - OBJETIVO E APLICAÇÃO

2.1. A presente Política estabelece princípios, diretrizes, processos e responsabilidades para o Gerenciamento de Riscos da Companhia e de suas Controladas, de modo a apoiar decisões informadas, proteger e gerar valor e contribuir para a continuidade dos negócios.

2.2. A presente Política aplica-se à Companhia, às suas Controladas e às Pessoas Abrangidas, na extensão de suas atribuições, de forma a possibilitar a adequada identificação, avaliação, direcionamento, monitoramento e comunicação dos Riscos aos quais a Companhia e suas Controladas estão ou podem ser expostas, contribuindo para o Gerenciamento de Riscos e para a tempestiva tomada de decisões e medidas aplicáveis.

CAPÍTULO III - DIRETRIZES E PROCESSOS DE GERENCIAMENTO DE RISCOS

3.1. O Gerenciamento de Riscos é responsabilidade de todos os Administradores e Colaboradores, e requer a participação ativa de todas as áreas da Companhia, na extensão de suas competências, integrando-se às metas e objetivos estratégicos dos negócios da Companhia e de suas Controladas.

3.2. A metodologia de Gerenciamento de Riscos observará, de forma proporcional à natureza e à complexidade dos negócios, as referências do COSO, da ABNT NBR ISO 31000 e do Instituto Brasileiro de Governança Corporativa, especialmente no que diz respeito ao fluxo de identificação, avaliação, tratamento e monitoramento dos Riscos aos quais a Companhia e suas Controladas estão expostas.

3.2.1. O sistema de gestão de riscos deve estimular todos os Administradores e Colaboradores a monitorar e fiscalizar os processos operacionais de forma preventiva, prospectiva e proativa no controle de riscos. A disseminação do conceito de risco é fundamental para que realizem suas atividades promovendo uma cultura de gerenciamento de riscos e ampliando o entendimento coletivo sobre os impactos que suas decisões e comportamentos podem gerar para os objetivos da Companhia.



3.2.2. O Gerenciamento de Riscos possui relacionamento direto com os objetivos da Companhia e de suas Controladas, impactando as estratégias de negócios, a definição de seus controles operacionais internos e a busca da excelência na gestão empresarial.

3.3. O Conselho de Administração aprovará a Matriz de Riscos, mediante recomendação do Comitê de Auditoria. A Diretoria e os Proprietários dos Riscos deverão conduzir os negócios observando a Matriz de Riscos aprovada.

3.4. O processo de Gerenciamento de Riscos compreenderá, no mínimo, as seguintes etapas:

(i) identificação e classificação dos Riscos conforme categorias descritas no item 4.1 abaixo;

(ii) análise dos Riscos identificados e indicação gráfica conforme a Matriz de Riscos abaixo:



(iii) definição e implementação das ações de resposta aos Riscos; e

(iv) definição dos procedimentos de monitoramento e comunicação.

3.5. A identificação e a análise de Riscos poderão utilizar, entre outras, as seguintes fontes e técnicas:

(i) Questionários e autoavaliações estruturadas: a liderança da Companhia é solicitada a preencher um questionário específico para que indique possíveis Riscos aos quais a Companhia está exposta, e os cenários de risco são observados e registrados;

(ii) Entrevistas: os cenários de riscos são identificados e discutidos com determinados Colaboradores, e os resultados também são documentados como parte da avaliação;

(iii) Auditorias de processos: os processos da Companhia são auditados e avaliados pela Auditoria Interna de forma independente, a fim de verificar eventuais Riscos aos quais está exposta. Neste processo, são elaboradas ou atualizadas matrizes de riscos e controles dos processos auditados. Tais registros contribuem para a identificação de Riscos dentro da Companhia, funcionando como uma fonte de possíveis ameaças ou fraquezas.

3.6. As etapas previstas no item 3.4 acima são finalizadas com o desenvolvimento de uma Matriz de Riscos. A Matriz de Riscos pode ser atualizada devido a: (i) novos cenários (interno, político, econômico, entre outros); (ii) resultados de auditorias, entrevistas, questionários, observações e demais atividades; ou (iii) evolução da cultura de integridade e mitigação de Riscos.

3.7. A análise dos Riscos identificados deverá considerar separadamente o Risco Inerente e o Risco Residual. Os critérios de Impacto deverão contemplar, conforme aplicável, dimensões financeiras, estratégicas, operacionais, legais, regulatórias, tecnológicas, ambientais, sociais, reputacionais e de continuidade; os critérios de Probabilidade deverão utilizar evidências históricas, exposição, vulnerabilidade e cenários prospectivos, conforme aplicável.

3.8. As respostas aos Riscos poderão consistir em: (i) terminar, ou seja, eliminar Riscos, redefinir os objetivos e/ou estratégias de negócios; (ii) diversificar, ou seja, intensificar o nível de gestão e/ou melhorar os controles internos; (iii) aceitar, ou seja, não realizar nenhuma ação adicional e continuar a monitorar o Risco, especialmente quando não é possível ou prático tratá-lo, nos termos do item 3.10; ou (iv) passar adiante, transferindo o impacto para terceiros (por exemplo, o custo do sinistro pode ser transferido para seguradoras).

3.9. Todo Plano de Ação deverá indicar, no mínimo, a medida de tratamento, o responsável e o prazo. O Proprietário do Risco responde pela implementação; a área de GRC monitora e escalona atrasos ou desvios; e a Auditoria Interna poderá avaliar a efetividade de forma independente.

3.10. A aceitação de Risco deverá ser fundamentada, com aprovação da Diretoria e ciência do Comitê de Auditoria. Riscos classificados como críticos na Matriz de Riscos ou suscetíveis de comprometer a continuidade dos negócios somente poderão ser aceitos, em caráter excepcional, pelo Conselho de Administração, após recomendação do Comitê de Auditoria, com prazo de revisão e monitoramento definidos pelo Proprietário do Risco.

3.11. A ocorrência de evento relevante ou a alteração material de exposição de Risco deverá ser comunicada imediatamente pelo Proprietário do Risco ao Diretor responsável e à área de GRC. Conforme a criticidade, a informação será escalonada ao Comitê de Auditoria e ao Conselho de Administração.

3.12. Riscos capazes de afetar a continuidade dos negócios deverão possuir estratégias de resposta, continuidade e recuperação proporcionais à criticidade, com responsáveis, canais de escalonamento e testes periódicos.

3.13. É recomendado que novos produtos, serviços, projetos, investimentos, operações societárias e alterações estratégicas materiais sejam precedidos de avaliação de Riscos compatível com sua natureza e submetidos às alçadas aplicáveis.

CAPÍTULO IV - CATEGORIAS DE RISCOS

4.1. Para fins de identificação, consolidação e reporte, os Riscos serão classificados, sem prejuízo de outras categorias que se mostrem necessárias, da seguinte forma:

(i) Riscos operacionais: relacionados a falhas ou inadequações de processos, pessoas, infraestrutura, fornecedores, continuidade, execução ou eventos externos que possam afetar as operações.

(ii) Riscos macroeconômicos e políticos: relacionados a alterações no ambiente econômico, político ou institucional, incluindo inflação, juros, emprego, renda, comportamento do consumidor, políticas públicas, instabilidade e eventos geopolíticos.

(iii) Riscos regulatórios e de compliance: relacionados ao descumprimento ou à alteração de leis, regulamentos, autorizações, compromissos, códigos e políticas aplicáveis, inclusive em matéria de integridade, prevenção a fraudes, corrupção e lavagem de dinheiro, que possam resultar em sanções, perdas financeiras, aumento de custos ou restrições às atividades da Companhia, inclusive à sua capacidade de investir em Bitcoin.

(iv) Riscos estratégicos: relacionados à formulação, execução ou revisão inadequada da estratégia, a premissas incorretas, à concorrência, à alocação de capital, a novos negócios, investimentos ou mudanças no modelo de negócios.

(v) Riscos jurídicos: relacionados a contratos, litígios, contingências, interpretações legais, direitos de terceiros e falhas na constituição, proteção ou exercício de direitos da Companhia.

(vi) Riscos tecnológicos, cibernéticos e de privacidade: relacionados a sistemas, infraestrutura, arquitetura, desenvolvimento, inteligência artificial, terceiros de tecnologia e segurança cibernética, que possam afetar a disponibilidade, a integridade ou a confidencialidade de dados e informações, tais como ciberataques,

indisponibilidade do ambiente de TI, obsolescência tecnológica, vazamento ou perda de dados pessoais e de informações estratégicas, envio indevido de arquivos confidenciais por meio digital ou telefônico, acesso inadequado a ativos e recursos de TI e acesso remoto inseguro, inclusive aqueles decorrentes de falhas na tecnologia ou na infraestrutura de Bitcoin que possam afetar a segurança dos ativos digitais da Companhia, resultando em perdas financeiras ou na impossibilidade de realizar transações de forma eficiente.

(vii) Riscos reputacionais e de imagem: relacionados a eventos, condutas ou percepções capazes de afetar a confiança e causar danos à reputação, imagem, credibilidade e/ou marca da Companhia e de suas Controladas, inclusive em razão de publicidade negativa, independentemente de sua veracidade, bem como aqueles relacionados à volatilidade do Bitcoin e possíveis perdas significativas que podem impactar negativamente a percepção do mercado.

(viii) Riscos ambientais, sociais e climáticos: relacionados a impactos, dependências e eventos ambientais, sociais ou climáticos, inclusive eventos físicos e de transição, direitos humanos, relações de trabalho e efeitos sobre pessoas, comunidades, operações e cadeia de valor.

(ix) Riscos financeiros: relacionados a mercado, crédito, contraparte, liquidez, capital, tesouraria, taxas de juros, câmbio, preços, concentração, instrumentos financeiros ou à insolvência de devedores, incluindo aqueles decorrentes das aplicações financeiras da Companhia em Bitcoin e derivativos.

CAPÍTULO V - RESPONSABILIDADES E COMPETÊNCIAS

5.1. A governança do Gerenciamento de Riscos compreende o Conselho de Administração, a Diretoria, o Comitê de Auditoria, a Auditoria Interna, a área de Governança, Riscos e Compliance (GRC), a área de Segurança da Informação, os Proprietários dos Riscos e as demais Pessoas Abrangidas, com atribuições distintas e atuação integrada, conforme a seguir.

5.2. Conselho de Administração. Compete ao Conselho de Administração da Companhia:

(i) aprovar esta Política de Gerenciamento de Riscos e suas alterações;

(ii) estabelecer as diretrizes gerais das estratégias de Gerenciamento de Riscos;

(iii) estabelecer o nível de risco a que a Companhia se submete na condução de seus negócios por meio da avaliação e aprovação da Matriz de Riscos apresentada pelo Comitê de Auditoria;

(iv) acompanhar e direcionar o desenvolvimento de uma sólida estrutura de Gerenciamento de Riscos, dando apoio em caso de necessidade aos demais integrantes da estrutura de Gerenciamento de Riscos da Companhia;

(v) assegurar ao Comitê de Auditoria autonomia operacional e orçamento próprio;

(vi) supervisionar as atividades do processo de Gerenciamento de Riscos executadas pelos demais integrantes da estrutura organizacional de Gerenciamento de Riscos da Companhia;

(vii) avaliar a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de Gerenciamento de Riscos;

(viii) acompanhar a evolução do Gerenciamento de Riscos;

(ix) aprovar as funções, o plano, a estrutura e o orçamento da Auditoria Interna e avaliar, ao menos anualmente, sua adequação, nos termos do Estatuto Social;

(x) deliberar sobre a aceitação excepcional de Riscos prevista no item 3.10;

(xi) acompanhar as conclusões da Auditoria Interna e a evolução das medidas corretivas relevantes;

(xii) monitorar o Comitê de Auditoria, bem como quaisquer outros Comitês de Assessoramento, estatutários ou não, integrantes da estrutura organizacional de Gerenciamento de Riscos da Companhia; e

(xiii) definir as decisões a serem tomadas nas hipóteses de conflitos e impasses, caso o Comitê de Auditoria (e, eventualmente, outros Comitês de Assessoramento integrantes da estrutura organizacional de Gerenciamento de Riscos) não chegue a uma decisão final sobre determinado tema.

5.3. Diretoria. Compete à Diretoria:

(i) implementar as estratégias e diretrizes aprovadas pelo Conselho de Administração, alocar recursos e assegurar a execução desta Política;

(ii) executar a Política de Gerenciamento de Riscos e, sempre que necessário, propor ao Conselho de Administração revisões às estratégias e diretrizes da Companhia ou à Política de Gerenciamento de Riscos; e

(iii) assegurar a designação dos Proprietários dos Riscos para identificar e avaliar os Riscos relevantes antes de decisões e iniciativas, nos termos do item 3.13, e escalonar tempestivamente ao Comitê de Auditoria e, conforme a criticidade, ao Conselho de Administração as exposições relevantes e os incidentes.

5.4. Comitê de Auditoria. Compete ao Comitê de Auditoria:

(i) avaliar e monitorar as exposições da Companhia, inclusive aquelas que possam afetar a continuidade dos negócios;

(ii) supervisionar as atividades das áreas financeira, controladoria e contábil da Companhia, avaliando as informações trimestrais e demonstrações financeiras;

(iii) supervisionar as atividades da Auditoria Interna e acompanhar a atuação da área de GRC;

(iv) opinar na contratação e destituição dos serviços de auditoria independente;

(v) avaliar a efetividade do modelo de Gerenciamento de Riscos e sugerir soluções de aprimoramento de seus processos ao Conselho de Administração, quando necessário, apontando as causas e responsabilidades;

(vi) recomendar ao Conselho de Administração a revisão ou a implementação de alterações, priorizações e inclusões na Matriz de Riscos, na distribuição de competências, nas categorias de Riscos, e nos processos internos de Gerenciamento de Riscos da Companhia;

(vii) recomendar ao Conselho de Administração a aceitação excepcional de Riscos prevista no item 3.10 e tomar ciência das demais aceitações de Risco;

(viii) assessorar o Conselho de Administração na avaliação de políticas, limites e Planos de Ação relacionados ao Gerenciamento de Riscos;

(ix) avaliar e monitorar o cumprimento e a efetividade desta Política e recomendar correções ou aprimoramentos necessários ao Conselho de Administração; e

(x) receber e tratar informações sobre descumprimentos legais, regulatórios e internos relevantes para suas atribuições.

5.4.1. O Comitê de Auditoria é órgão vinculado ao Conselho de Administração, dotado de autonomia operacional e orçamento próprio aprovado pelo Conselho de Administração, destinado a cobrir despesas com seu funcionamento.

5.4.2. O Comitê de Auditoria observará seu regimento interno e o Regulamento do Novo Mercado, sem assumir responsabilidades próprias da Diretoria ou dos Proprietários dos Riscos.

5.5. Auditoria Interna. Compete à Auditoria Interna, própria ou exercida por auditor independente contratado para essa finalidade:

(i) avaliar, com independência e objetividade, a qualidade e a efetividade do Gerenciamento de Riscos, dos controles internos e da governança;

(ii) executar plano de auditoria baseado em Riscos, aprovado pelo Conselho de Administração, mediante recomendação do Comitê de Auditoria;

(iii) reportar funcionalmente ao Conselho de Administração, diretamente ou por meio do Comitê de Auditoria, conclusões e recomendações independentes e tempestivas;

(iv) executar testes de controles de acordo com o planejamento da auditoria;

(v) identificar e recomendar melhorias nos processos de controles internos e de gestão de Riscos, sem assumir a gestão dos Riscos, a execução dos controles ou a responsabilidade pelos Planos de Ação;

(vi) emitir opinião formal sobre os controles internos testados;

(vii) verificar, de forma independente, a implementação dos Planos de Ação decorrentes de seus trabalhos; e
(viii) comunicar prontamente deficiências relevantes, agravamentos de Risco e atrasos críticos ao Comitê de Auditoria.

5.5.1. As funções, o plano, a estrutura e o orçamento da Auditoria Interna serão aprovados pelo Conselho de Administração, que avaliará sua adequação ao menos uma vez ao ano.

5.6. Área de Governança, Riscos e Compliance (GRC). Compete à área de GRC:
(i) identificar, avaliar e monitorar os Riscos apresentados no item 4.1 acima, conforme aplicável;
(ii) buscar identificar fragilidades nos processos e controles internos da Companhia, por meio de avaliações dos procedimentos e práticas adotadas nas demais áreas;
(iii) reportar qualquer evento ou situação que possa comprometer a governança, a conformidade ou a gestão de Riscos da Companhia à Diretoria e ao Comitê de Auditoria;
(iv) recomendar Planos de Ação e controles para mitigar os Riscos decorrentes das fragilidades identificadas nos processos e controles internos da Companhia;
(v) acompanhar e monitorar a implementação de Planos de Ação para mitigar os Riscos identificados, seja pela própria área de GRC ou pelo trabalho da Auditoria Interna; e
(vi) orientar as áreas, promover a cultura de Riscos e propor aprimoramentos desta Política e da metodologia.

5.7. Área de Segurança da Informação. Compete à área de Segurança da Informação:
(i) identificar, monitorar e mitigar os Riscos relacionados ao ambiente de tecnologia da informação (infraestrutura, gestão de acessos, segurança da informação, privacidade) que possam prejudicar ou impedir o bom andamento das operações da Companhia, tais como ciberataques, destruição de servidores, restrição de acesso aos sistemas de informação, perda de informações relevantes, dentre outros;
(ii) buscar identificar fragilidades nos recursos e procedimentos empregados pela Companhia no tratamento de informações, por meio de inspeções periódicas aos parâmetros e recursos tecnológicos disponíveis;
(iii) implementar Planos de Ação e controles aos Riscos decorrentes das fragilidades identificadas nos recursos e procedimentos empregados pela Companhia no tratamento de informações, conforme aplicável;
(iv) recomendar as ações a serem implementadas para o tratamento dos Riscos em relação ao ambiente de tecnologia da informação, sem afastar a responsabilidade dos Proprietários dos Riscos;
(v) reportar qualquer evento relacionado ao ambiente de tecnologia da informação que possa prejudicar ou impedir o bom andamento das operações da Companhia e comunicar tempestivamente exposições relevantes à Diretoria e à área de GRC; e
(vi) realizar avaliações, testes e monitoramentos especializados compatíveis com suas atribuições.

5.8. Proprietários dos Riscos, gerências e demais Colaboradores. Compete-lhes, na extensão de suas atribuições:
(i) observar integralmente as ações de Gerenciamento de Riscos no dia a dia da Companhia;
(ii) identificar, avaliar, registrar e monitorar os Riscos de seus processos, manter controles e evidências e observar esta Política;
(iii) implementar e executar os controles e os Planos de Ação sob sua responsabilidade, acompanhar indicadores (conforme aplicável) e comunicar atrasos, desvios e mudanças de exposição;
(iv) reportar tempestivamente eventos e informações relevantes ao Diretor responsável e à área de GRC; e
(v) participar de forma ativa na comunicação e treinamento que permita a disseminação de forma consciente do Gerenciamento de Riscos na Companhia.

5.9. Os controles internos contribuem para a mitigação dos Riscos, propiciando um ambiente mais seguro e

eficaz, no que tange à eficiência operacional e à integridade dos registros e informações, considerando principalmente os seguintes aspectos:

(i) os objetivos estratégicos da Companhia;
(ii) a confiabilidade e a integridade das informações financeiras;
(iii) a conformidade com obrigações legais, regulatórias, contratuais e internas e a proteção de ativos; e
(iv) a prevenção e a detecção tempestiva de erros, fraudes, incidentes e perdas.

5.10. O Gerenciamento de Riscos adota o Modelo das Três Linhas, preservadas as responsabilidades do Conselho de Administração, do Comitê de Auditoria e da Diretoria:

- **1ª Linha:** composta pelos Proprietários dos Riscos, gerências e demais Colaboradores que atuam nas operações da Companhia, responsáveis por identificar, avaliar e monitorar os Riscos de seus processos, implementar e executar os controles e os Planos de Ação sob sua responsabilidade e fornecer informações completas e tempestivas à Diretoria e à segunda linha;
- **2ª Linha:** composta pela área de GRC, pela área de Segurança da Informação e por outras funções especializadas de controle, responsáveis por estabelecer metodologias, orientar, monitorar e reportar, sem acumular atividades operacionais que possam comprometer sua objetividade; e
- **3ª Linha:** Auditoria Interna, responsável por fornecer avaliação independente ao Conselho de Administração, diretamente ou por meio do Comitê de Auditoria, sobre a efetividade da governança, do Gerenciamento de Riscos e dos controles internos.

5.11. Os processos, Riscos e controles deverão ser documentados e atualizados periodicamente, e sempre que houver mudança ou incidente relevante.

5.12. Os controles inexistentes ou considerados insatisfatórios para mitigação dos Riscos identificados são reportados para as áreas responsáveis pela elaboração de Planos de Ação (seja a criação do novo controle ou o aperfeiçoamento dos controles existentes).

5.13. Deficiências de controle deverão ser classificadas segundo sua relevância, atribuídas ao responsável e tratadas por Plano de Ação com prazo definido. Atrasos serão escalonados conforme esta Política.

5.14. A Auditoria Interna considerará o universo de Riscos e controles em seu planejamento baseado em Riscos, preservada sua independência para definir escopo, procedimentos, amostras e conclusões.

CAPÍTULO VI - VIGÊNCIA

6.1. A primeira versão desta Política foi aprovada em Reunião do Conselho de Administração realizada em 5 de outubro de 2020, e a segunda versão foi aprovada em 6 de agosto de 2024.

6.2. A presente versão desta Política foi aprovada pelo Conselho de Administração da Companhia em 04 de novembro de 2026, entrando em vigor na mesma data e permanecendo vigente por prazo indeterminado.

6.3. Esta Política deverá ser revisada sempre que houver alteração legal, regulatória, estatutária, estratégica ou operacional relevante. Qualquer alteração desta Política somente poderá ser aprovada pelo Conselho de Administração.

CAPÍTULO VII - DISPOSIÇÕES GERAIS

7.1. As Pessoas Abrangidas deverão preservar o sigilo das informações a que tenham acesso em razão desta Política, observadas as regras internas, a confidencialidade a respeito dos temas relativos a suas atividades e as exceções de compartilhamento autorizado ou exigido por lei, regulamentação, ordem de autoridade

competente ou dever de divulgação da Companhia.

7.2. Dúvidas operacionais acerca desta Política serão tratadas pela área de GRC. Questões de interpretação, casos omissos e exceções materiais serão submetidos ao Comitê de Auditoria e, conforme a relevância ou a competência, ao Conselho de Administração.

7.3. O inteiro teor desta Política será divulgado no website de relações com investidores da Companhia (ri.meliuz.com.br) e nos sistemas da CVM, conforme aplicável.

7.4. O descumprimento desta Política será apurado pelas instâncias competentes e poderá resultar nas medidas disciplinares, societárias, contratuais, civis e administrativas cabíveis, observados a legislação e os normativos internos aplicáveis.

ANEXO I

TERMO DE ADESÃO

Declaro que recebi, li e compreendi a Política de Gerenciamento de Riscos do Méliuz S.A. e comprometo-me a cumprir suas disposições, a comunicar tempestivamente os Riscos e eventos relevantes de que tenha conhecimento e a participar dos treinamentos aplicáveis. Estou ciente de que o descumprimento poderá resultar nas medidas cabíveis. Este Termo poderá ser assinado física ou eletronicamente.

Nome completo:

CPF:

Data:

Assinatura: