POLÍTICA DE GERENCIAMENTO DE RISCOS DA COBASI COMÉRCIO DE PRODUTOS BÁSICOS E INDUSTRIALIZADOS S.A.

1. OBJETIVO

A Cobasi Comércio de Produtos Básicos e Industrializados S.A. ("Companhia"), com a finalidade de trazer maior segurança a seus acionistas e à continuidade de seu negócio, apresenta sua Política de Gerenciamento de Riscos ("Política"), de modo a formalizar e divulgar os princípios, diretrizes e responsabilidades para fins de identificação, controle e mitigação dos riscos aos quais a Companhia está exposta.

A Política tem o objetivo de ser um mecanismo para auxiliar na identificação, avaliação, previsão e monitoramento dos riscos aos quais a Companhia está sujeita, padronizando as atividades de controle e de gerenciamento dos riscos que devem ser desempenhadas em todos os níveis da Companhia e nos estágios de seus processos corporativos.

2. ABRANGÊNCIA

A Política é aplicável à Companhia em todos os seus macroprocessos e operações, sendo obrigatória a sua observância por seus respectivos colaboradores e administradores.

3. REFERÊNCIAS

A Política foi moldada e baseada fundamentalmente: (i) nas recomendações de normas de gerenciamento de risco empresarial reconhecidas no mercado; e (ii) no Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão ("B3").

4. CATEGORIAS DE RISCOS

4.1. Riscos Estratégicos

Os riscos estratégicos são aqueles associados à estratégia da Companhia na busca de criação, proteção e crescimento de valor. São causados por mudanças no ambiente externo, tais como político, econômico e social, mercado, competidores, fusões e aquisições, reputação e imagem, disponibilidade de recursos e alterações nas regras aplicáveis ao mercado.

4.2. Riscos Operacionais

Os riscos operacionais são aqueles decorrentes da inadequação ou falha na gestão de processos internos e de pessoas, que possam dificultar ou impedir o alcance dos objetivos da Companhia. Eles estão associados tanto à operação do negócio (como na distribuição, marketing e vendas), quanto à gestão de áreas de suporte ao negócio (como contabilidade, controles, suprimentos e gestão de capital humano). Também inclui indenizações por danos

causados a terceiros decorrentes das atividades da Companhia (como advindos de relações de consumo) e fraudes internas e externas (como furto de estoque de materiais e medicamentos).

4.3. Riscos Financeiros

Os riscos financeiros são aqueles decorrentes de efeitos inesperados no cenário econômico, político e nas tendências de mercado, que podem refletir no comportamento do consumidor, na taxa de juros, inflação, investimentos financeiros, dentre outros, podendo englobar riscos de mercado, de crédito e de liquidez.

4.4. Riscos de Conformidade

Os riscos legais e de conformidade são os riscos de imposição de sanções legais ou regulatórias, de perda financeira ou de reputação, que a Companhia pode sofrer como resultado do descumprimento de leis, acordos, normas e regulamentos, bem como de suas próprias políticas e procedimentos internos. Também incluem os riscos no âmbito de processos trabalhistas e de questões tributárias, de fraudes em demonstrações financeiras e de desvios de ativos, de corrupção, entre outros.

4.5. Riscos da Informação

Os riscos de informação são aqueles que consistem na perda, uso indevido, acesso ou divulgação não autorizada de informações ou dados pessoais de partes interessadas, internas ou externas, podendo ameaçar os negócios ou prejudicar a imagem da Companhia.

4.6. Riscos ESG

Os riscos de ESG (Environmental, Social and Governance) são aqueles relacionados a fatores ambientais, sociais e de governança que podem impactar a estratégia, operações e reputação de uma organização.

4.7. Riscos Tecnológicos

Os riscos de tecnologia são aqueles referentes a falha sem sistemas de TI, ataques cibernéticos, vazamentos de dados ou interrupções nos sistemas críticos podem paralisar as operações e comprometer a segurança da informação.

4.8. Riscos de Terceiros

Os riscos de terceiros são aqueles referentes a falhas ou problemas com fornecedores, prestadores de serviços ou parceiros de negócios que afetam a cadeia de suprimentos, qualidade dos produtos ou serviços prestados.

4.9. Riscos de Reputação

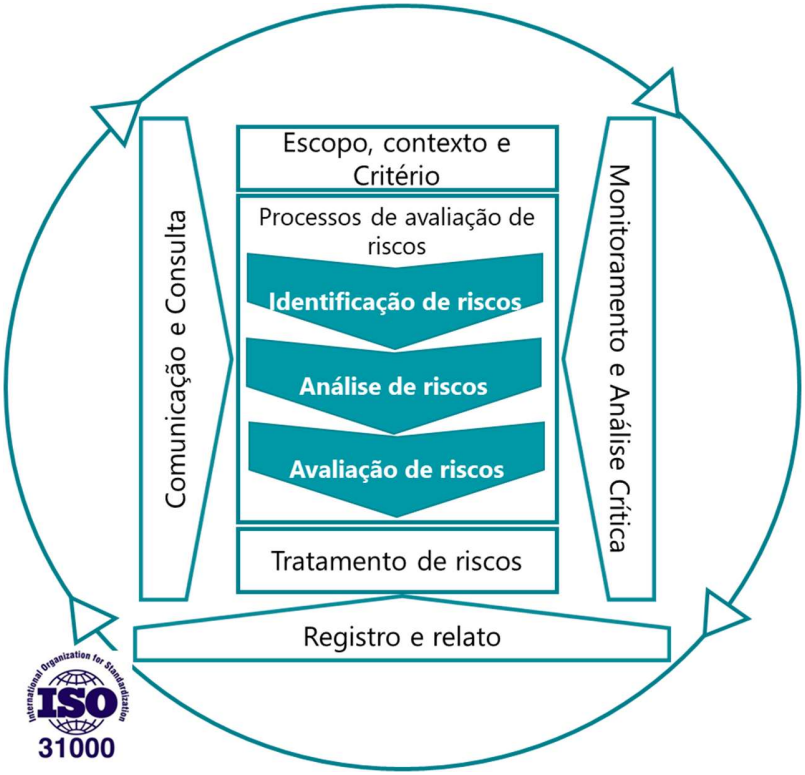
Os riscos de reputação são aqueles relacionados a questões de imagem pública, como crises de comunicação, podem causar danos à reputação da empresa, afetando sua confiança no mercado e nas relações com stakeholders.

5. DIRETRIZES

A Companhia identifica e trata os riscos a que está exposta de forma a garantir o cumprimento das metas estabelecidas em seu planejamento estratégico.

5.1. Processo de Gerenciamento de Riscos

O processo de gerenciamento de Riscos adotado pela Companhia foi elaborado à luz do disposto no “ISO 31000:2018 – Princípios e Diretrizes da Gestão de Riscos”:



5.2. Identificação e Classificação do Risco

Nesta etapa, a Companhia identifica eventos que podem impactar seus objetivos e estratégia. Os riscos aos quais a Companhia está exposta podem ser identificados por meio de uma série de instrumentos, incluindo:

- **Ciclos de entrevistas.** Os cenários de risco são identificados e discutidos com determinados colaboradores da Companhia. Os resultados também são documentados como parte da avaliação; e

- **Auditorias de processos.** Os processos da Companhia são auditados e avaliados, a fim de verificar eventuais riscos aos quais está exposta. Neste processo, matrizes de riscos são criadas ou atualizadas. Tais registros contribuem para a identificação de riscos dentro da Companhia, funcionando como uma fonte

de possíveis ameaças/fraquezas.

Após a coleta das informações por meio desses instrumentos, a Companhia desenvolve um Mapa de Riscos, avaliado anualmente pelo Comitê de Auditoria. Os riscos descritos no Mapa de Riscos poderão ser atualizados considerando os seguintes aspectos:

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.

5.3. Análise de Riscos

Uma vez realizada a identificação e classificação dos riscos, são definidos aqueles que apresentam maior relevância para tratamento. Para análise são considerados os seguintes aspectos:

- **Impacto/consequência** que o risco identificado pode gerar, tais como, potencial de perdas financeiras, degradação da imagem, penalidades legais, entre outros resultados negativos; e

- **Probabilidade/vulnerabilidade** da ocorrência, considerando a complexidade e robustez dos controles internos existentes para aquele risco.

O perfil do risco é definido:

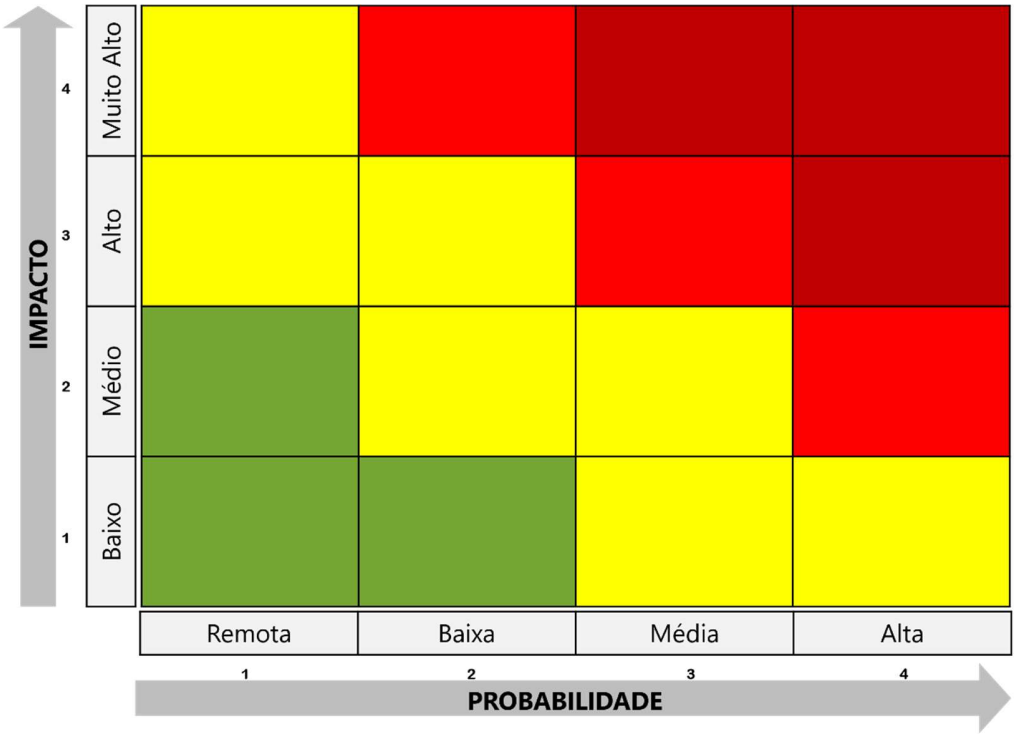
- Pela combinação dos dois aspecto (impacto x probabilidade).
- Pontuação média ponderada (1 a 4).
- Score Médio do agrupamento.

5.4. Processo de Avaliação

A avaliação dos riscos é realizada, principalmente, de acordo com o previsto abaixo:

- Identificação dos fatores (causas) de riscos e implicações nos objetivos (metas e resultados) projetados;

- Análise dos principais riscos suscetíveis de afetar os seus objetivos, por meio da determinação do grau de impacto e probabilidade de ocorrência dos Riscos, conforme Mapa de Risco abaixo:



- Priorização e definição do limite (ou apetite) de cada risco que a Companhia e seus acionistas estão dispostos a correr na busca pelo retorno e geração de valor, classificando os riscos como de acordo com a matriz de priorização de riscos e as definições abaixo:

- **I - Risco Muito Alto:** Riscos são inaceitáveis e demandam ação gerencial prioritária para eliminar a componente de risco ou reduzir sua severidade e/ou probabilidade de ocorrência.

- **II - Risco Alto:** Riscos inesperados, com alto impacto e baixa probabilidade de

ocorrência. Riscos 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.

- **III - Risco Moderado:** Riscos de menor criticidade devido ao menor nível de impacto no valor do negócio – 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. Tratamento sujeito à viabilidade de contratação de seguros como resposta a estes riscos.

- **IV - Risco Baixo:** Riscos de baixo impacto e probabilidade de ocorrência, não havendo necessidade de monitoramento contínuo.

5.5. Tratamento de Riscos

A partir dos riscos identificados, avaliados e analisados, a Companhia define e recomenda ações de respostas, considerando as seguintes hipóteses:

i. **Evitar o risco**, ou seja, eliminar a causa raiz e redefinir os objetivos e/ou estratégias de negócios;

ii. **Reduzir o risco**, ou seja, intensificar o nível de gestão e/ou melhorar os controles internos, diminuindo as causas ou consequencias;

iii. **Aceitar o risco**, ou seja, não realizar nenhuma ação adicional e continuar o monitorando, especialmente quando não é possível ou prático respondê-lo (situações em que o custo da ação mitigatória ultrapasse a exposição ao risco); ou

iv. **Compartilhar o risco**, transferindo total ou parcial a responsabilidade para terceiros (e.g. no risco de incêndio, o custo do sinistro pode ser transferido para seguradoras).

Tais recomendações se desdobram em ações detalhadas, pilotos, testes, validações e ajustes necessários para assegurar a eficácia do tratamento e controle dos riscos aos quais a Companhia está exposta.

A partir da definição dos riscos e das recomendações dadas pela Controladoria, as áreas de negócio da Companhia devem implementar os planos de ação a fim de garantir o devido tratamento. A implementação das atividades, ações e prazos de resposta são acompanhados pela Controladoria e reportados periodicamente à Diretoria Executiva.

As ferramentas utilizadas no processo de tratamento dos riscos devem objetivar sua (i) eliminação, (ii) mitigação ou (iii) transferência à terceiros.

5.6. Monitoramento e Comunicação

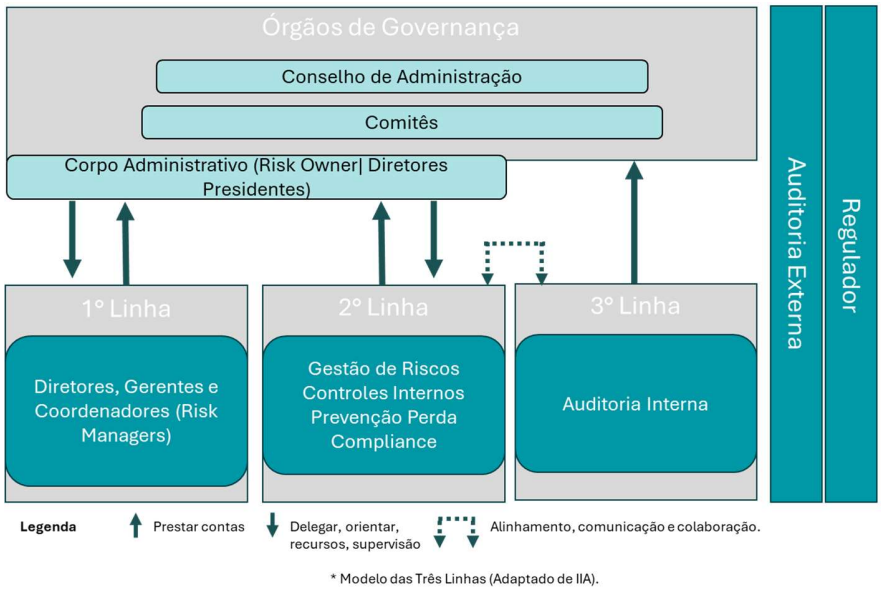
A área de Auditoria Interna é responsável por aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, fornecendo relatórios periódicos ao Comitê de Auditoria, a fim de garantir que a cultura de transparência, responsabilização e

conscientização sobre os riscos está sendo devidamente implementada pelo Jurídico.

A partir da identificação dos Riscos, estes deverão ser monitorados de forma contínua, de acordo com a divisão de responsabilidades descrita no item 6 abaixo.

6. RESPONSABILIDADES

Seguindo o modelo de “Três Linhas”, o gerenciamento dos Riscos deve ser realizado sob a responsabilidade dos órgãos de governança, gestores e responsáveis diretos pelos processos, conforme descrito neste item.



* Modelo das Três Linhas (Adaptado de IIA).

- 1ª linha: São responsáveis por gerenciar os riscos de sua área, conduzir ações para mitigação dos riscos e ter propriedade sobre eles. Devem manter processos apropriados, garantindo a conformidade com as expectativas legais, regulatórias e éticas.
- 2ª linha: Tem como objetivo apoiar a primeira linha, com expertise complementar incluindo a melhoria continua das práticas de gestão de riscos nos níveis de processos e sistemas, fornecendo análises e reportando as adequações necessárias.
- 3ª linha: Tem como objetivo uma avaliação objetiva e independente da gestão de riscos, identificando controles necessários a serem implementados.

6.1. Conselho de Administração

É responsável pela governança do processo de gerenciamento de riscos, e tem como atribuições:

i. Aprovar a presente Política, diretrizes, Mapa de Riscos e suas eventuais alterações;

ii. Definir uma tolerância de risco apropriada, priorizando riscos e aprovando planos de mitigação;

iii. Supervisionar e aprovar planos de resposta a riscos, quando necessário;

iv. Fornecer à Diretoria Executiva, quando necessário, sua percepção do grau de exposição a riscos que a Companhia está exposta (visão do acionista) e influenciar na priorização dos riscos a serem tratados; e

v. Avaliar a adequação da estrutura operacional e de controles internos para o gerenciamento de riscos.

6.2. Diretoria Executiva

i. Desenhar as diretrizes, mapa de risco, determinando os limites de exposição, impactos, e a tolerância de exposição aos riscos;

ii. Definir a estrutura para o sistema de gerenciamento de riscos dentro da Companhia;

iii. Definir, em conjunto com as áreas de Controladoria, Jurídico, Auditoria Interna, conforme aplicável, e o Comitê de Auditoria, os planos de ação para mitigação dos Riscos;

iv. Supervisionar o processo de avaliação de riscos e monitorar os sistemas de gerenciamento de risco; e

v. Disseminar a cultura da gestão de risco em toda Companhia.

6.3. Comitê de Auditoria

i. Avaliar e monitorar a exposição da Companhia a riscos que possam afetar a sua sustentabilidade;

ii. Acompanhar e supervisionar as atividades de gerenciamento de riscos do Jurídico, da Controladoria e da área de Auditoria Interna;

iii. Avaliar a efetividade do modelo de gestão de riscos da Companhia;

iv. Sugerir soluções de aprimoramento dos processos internos de gerenciamento de riscos a Diretoria Executiva, incluindo, mas não se limitando, a Políticas de Transações entre Partes Relacionadas da Companhia;

v. Recomendar a Diretoria Executiva a revisão ou implementação de alterações, priorizações e inclusões à Mapa de Riscos da Companhia;

vi. Opinar na contratação e destituição dos serviços de auditoria independente;

vii. Emitir anualmente relatório resumido contemplando as reuniões realizadas e os principais assuntos discutidos, destacando as recomendações feitas para a Diretoria Executiva e o Conselho de Administração; e

viii. Informar trimestralmente ao Conselho de Administração sobre suas atividades, observado que a ata da reunião deverá ser divulgada.

6.4. Área de Auditoria Interna

i. Aferir a qualidade e a efetividade dos processos de gerenciamento de riscos fornecendo relatórios periódicos ao Comitê de Auditoria e sugerindo alterações ao Conselho de Administração e à Diretoria Executiva;

ii. Fornecer, quando solicitado, informações precisas, íntegras e suficientes para a modelagem de riscos;

iii. Apresentar, quando solicitado, sua percepção quanto à exposição ao Risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado; e

iv. Propor limites aos riscos à Diretoria Executiva.

Alternativamente à constituição de área própria de auditoria interna, a Companhia poderá contratar auditor independente registrado na CVM, responsável por essa função.

6.5. Gestores das áreas de negócios e responsáveis diretos pelos processos, como primeira linha de defesa, com reporte à Diretoria Executiva

i. Identificar e gerenciar os riscos das respectivas áreas de negócio e processos de acordo com os limites de riscos;

ii. Comunicar, tempestivamente, à área de Auditoria Interna e a área de Controladoria da Companhia, os eventos de risco que apresentarem tendência de ocorrência e/ou eventual extrapolação dos limites de risco; e

iii. Implementar e acompanhar os planos de ação para mitigação de riscos e acompanhar as ações corretivas nas respectivas áreas e processos.

6.6. Áreas de Controladoria e Jurídico, em conjunto, como segunda linha de defesa, com reporte à Diretoria Executiva

i. Administrar o sistema de gerenciamento de risco;

ii. Fornecer apoio metodológico aos departamentos operacionais e funcionais da Companhia por meio de ferramentas e serviços sob demanda;

iii. Fornecer informações precisas, íntegras e suficientes para a modelagem de riscos;

iv. Apresentar percepção quanto à exposição ao risco (magnitude de impacto e probabilidade de ocorrência), se possível, pautada também em indicadores de mercado;

v. Propor limites para exposição aos riscos e sugerir, avaliar, implantar e monitorar as ações com o objetivo de reduzir a exposição ao risco;

vi. Supervisionar o processo de avaliação de riscos em conjunto com a Diretoria Executiva e assegurar monitoramento constante de riscos de fontes externas, com visão prospectiva sobre os riscos emergentes;

vii. Acompanhar a Diretoria Executiva na implantação desta Política por meio da disseminação de ferramentas e boas práticas;

viii. Avaliar os riscos associados a certos projetos estratégicos, parcerias ou transações de fusões e aquisições;

ix. Cumprir os limites de riscos aprovados pelo Conselho de Administração;

x. 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

xi. Assegurar as informações disponibilizadas à Diretoria Executiva sobre riscos ou incidentes, bem como coordenar o sistema de gerenciamento dos riscos em momentos de crises em caso de grandes acontecimentos.

As funções de *Compliance* da Companhia são exercidas pela área Jurídica, enquanto as atividades de controles internos e riscos é exercida pela área de Controladoria. Os membros dessas áreas não podem acumular funções com atividades operacionais.

7. DISPOSIÇÕES GERAIS

As regras referentes ao Regulamento do Novo Mercado constantes desta Política somente terão eficácia a partir da data da entrada em vigor do Contrato de Participação no Novo Mercado e da admissão dos valores mobiliários da Companhia à negociação em mercado de bolsa por entidade administradora de mercado organizado.

8. VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação e pode ser consultada em https://ri.cobasi.com.br/ e https://cvmweb.cvm.gov.br.