

**POLÍTICA DE GERENCIAMENTO DE RISCOS**  
**DA CANTU STORE S.A**

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|  CantuStore  | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>2/16                         | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

## ÍNDICE

|   |    |
|---|----|
| <b>1. OBJETIVO</b> .....                                  | 3  |
| <b>2. REFERÊNCIAS</b> .....                               | 3  |
| <b>3. ABRANGÊNCIA</b> .....                               | 3  |
| <b>4. DEFINIÇÕES</b> .....                                | 3  |
| <b>5. RESPONSABILIDADES</b> .....                         | 4  |
| <b>6. RISCOS AOS QUAIS A COMPANHIA ESTÁ EXPOSTA</b> ..... | 10 |
| <b>7. DIRETRIZES</b> .....                                | 11 |
| <b>8. METODOLOGIA</b> .....                               | 12 |
| <b>9. DISPOSIÇÕES GERAIS</b> .....                        | 16 |
| <b>10. DOCUMENTOS COMPLEMENTARES</b> .....                | 16 |

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>3/16                 | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

## 1. OBJETIVO

A presente Política de Gerenciamento de Riscos (“Política”), aprovada na reunião do Conselho de Administração da Cantu Store S.A (“Companhia”) realizada em 20 de outubro 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, a avaliação, o tratamento, o monitoramento e a comunicação de Riscos inerentes às atividades da Companhia e que possam afetar o atendimento aos seus objetivos e realização de seus negócios.

## 2. REFERÊNCIAS

Esta Política tem como referências:

- (i) as diretrizes de governança corporativa do estatuto social da Companhia;
- (ii) as normas aplicáveis emanadas pela Comissão de Valores Mobiliários (“CVM”);
- (iii) o Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão;
- (iv) as diretrizes e princípios descritos no Código de Conduta da Companhia;
- (v) o benchmarking do mercado, principalmente com relação ao setor de atuação da Companhia; e
- (vi) o modelo do COSO-ERM - Committee of Sponsoring Organizations of Treadway Commission (“COSO-ERM”).

## 3. ABRANGÊNCIA

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

## 4. DEFINIÇÕES

Limite (do Risco): 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: avaliação do retorno tangível e intangível relacionado ao Limite de Risco proposto; capacidade da Companhia de suportar o impacto do Limite de Risco proposto; decisão se o Risco deve ou não ser aceito conforme sua tipologia; viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e disponibilidade de recursos (investimento e esforço) para implantação;

Mapa de Riscos: mapa de Riscos classificados em 6 (seis) principais macro-categorias: estratégicos (que dentre outros engloba o risco político); operacionais; financeiros; conformidade e regulatório;

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>4/16                 | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

tecnológicos; socioambientais – os quais, de forma conjunta, compreendem as categorias dos Riscos da Companhia;

*Matriz de Riscos:* visa a 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, pela Área de Compliance, Gerenciamento de Riscos e Controles Internos, por ocasião da revisão de planejamento estratégico da Companhia e, tempestivamente, com o surgimento de eventos de Risco emergentes, conforme percepção de impacto e probabilidade pelo Comitê de Auditoria e posteriormente validada pelo Conselho de Administração da Companhia;

*Proprietário(s) do Risco:* colaboradores da Companhia que possuem o maior domínio e conhecimento técnico acerca do Risco correspondente à área de atuação, responsáveis pela tomada de decisão e capazes de estabelecer e gerir os planos de ação para adequar a exposição aos Limites aprovados;

*Risco(s):* todo e qualquer evento decorrente de incertezas a 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. RESPONSABILIDADES

Esta Política define e comunica os papéis e responsabilidade dos principais agentes envolvidos no processo de gestão de Riscos, desenhados na busca pela construção e implantação de um modelo que capture as experiências, as percepções e os melhores conjuntos de informações disponíveis para a tomada de decisão.

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 (*Enterprise Risk Management*). 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:

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

*2ª Linha de Defesa:* é representada pelas funções de gerenciamento de Riscos, Controles Internos e de Compliance – exercidas pela Área de Compliance, Gerenciamento de Riscos e Controles Internos da Companhia –, que atua na garantia do apropriado funcionamento da primeira linha, por meio do estabelecimento de controles, identificação de falhas de performance de controles e identificação de desvios de políticas e procedimentos internos. Área de Compliance, Gerenciamento de Riscos e Controles Internos se reporta ao Comitê de Auditoria, e pode contar com o auxílio de outras áreas da Companhia, tais como jurídico e recursos humanos, para o desempenho de suas atividades.

*3ª Linha de Defesa:* é representada pela função de Auditoria Interna – exercida por auditor independente registrado na CVM, contratado pela Companhia –, que atua no fornecimento de

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>5/16                 | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

avaliações independentes à administração, especialmente pela realização de testes substantivos de controles internos para identificação de desvios operacionais e financeiros decorrentes de falhas, deficiências e/ou fraudes.

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

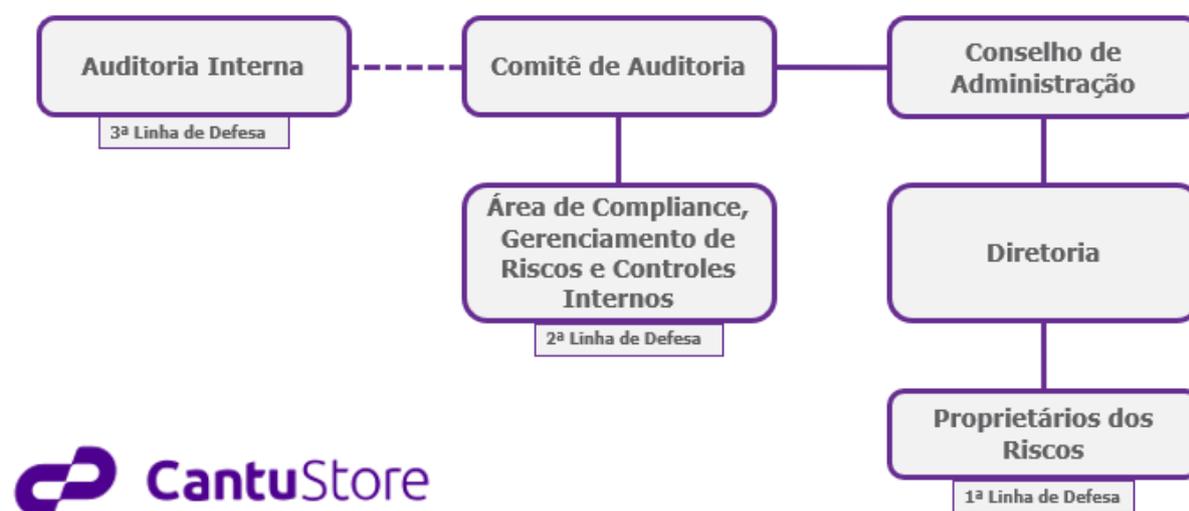


Figura 1. Estrutura de Gerenciamento de Riscos da Companhia

O Conselho de Administração tem competência para monitorar o funcionamento do processo de gestão, acompanhar o perfil de Riscos da Companhia e os planos de ação definidos em resposta aos Riscos. Nesse contexto, compete ao Conselho de Administração da Companhia:

- (i) Definir os objetivos estratégicos, as diretrizes, o perfil e o Limite de Riscos da Companhia, adequados e aderentes aos seus negócios;
- (ii) Aprovar políticas, diretrizes, o Mapa e a Matriz de Risco, Limites de Riscos e impactos propostos;
- (iii) Fornecer, periodicamente, sua percepção do grau de exposição a Riscos a que a Companhia está exposta e influenciar na priorização dos Riscos a serem tratados;
- (iv) Assegurar ao Comitê de Auditoria plena autonomia operacional, aprovando-lhe orçamento próprio destinado e adequado a cobrir despesas com seu funcionamento;
- (v) Aprovar a contratação ou destituição dos serviços de auditoria independente, com o suporte do Comitê de Auditoria; e

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|    | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>6/16                         | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

- (vi) Receber, diretamente ou por meio do Comitê de Auditoria, o reporte das atividades de auditoria interna exercidas por auditores independentes registrados na CVM.

Compete ao Comitê de Auditoria da Companhia, órgão autônomo de assessoramento vinculado ao Conselho de Administração, entre outras atribuições previstas em seu Regimento Interno:

- (i) Aprovar e/ou sugerir melhorias no planejamento de auditoria interna;
- (ii) Avaliar e monitorar as exposições de Risco da Companhia, para desenvolvimento de ações que promovam redução de Riscos e ameaças;
- (iii) Recomendar ao Conselho de Administração da Companhia a avaliação de políticas, Limites e planos de ação;
- (iv) Avaliar, monitorar, e recomendar à administração a correção ou o aprimoramento das políticas internas da companhia, incluindo a política de transações entre partes relacionadas;
- (v) Monitorar o cumprimento desta Política e avaliar a sua aplicabilidade frente aos Limites de Risco aprovados;
- (vi) Opinar na contratação e destituição dos serviços de auditoria independente;
- (vii) Avaliar a efetividade do modelo de gestão de Riscos e sugerir aprimoramentos ao processo, apontando as causas e responsabilidades;
- (viii) Acompanhar as atividades da auditoria independente e da área de Compliance, Gerenciamento de Riscos e Controles Internos da Companhia, reportando-as ao Conselho de Administração; e
- (ix) Receber e tratar, junto à Área de Compliance, Gerenciamento de Riscos e Controles Internos, as informações acerca do descumprimento de dispositivos legais e normativos aplicáveis à Companhia, além de regulamentos e códigos internos, e inclusive estabelecer procedimentos específicos para proteção do prestador e da confidencialidade da informação;

Compete à Diretoria da Companhia, enquanto órgão colegiado:

- (i) Atualizar o Mapa de Riscos sempre que ocorrer a revisão do plano estratégico e tempestivamente com o surgimento de fatores de Risco emergentes;
- (ii) Estabelecer a priorização dos Riscos a partir do impacto e probabilidade, visando a definir 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, recomendando ações de respostas;

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|    | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>7/16                         | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

- (iv) Acompanhar periodicamente 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, inclusive por meio de incentivos.

Compete à função de *Auditoria Interna*, exercida por auditores independentes registrados na CVM e contratados pela Companhia – que reporta suas atividades ao Conselho de Administração por meio do Comitê de Auditoria:

- (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 periódicos ao Comitê de Auditoria, a fim de garantir que os processos e a estrutura de gerenciamento de Riscos estejam sendo devidamente obedecidos.

Compete à *Área de Compliance, Gerenciamento de Riscos e Controles Internos* exercer as funções de compliance, riscos corporativos e controles internos da Companhia, e os seus colaboradores não acumulam funções nem possuem relação de subordinação com áreas operacionais. No que diz respeito ao gerenciamento de riscos e controles internos, a Área de Compliance, Gerenciamento de Riscos e Controles Internos tem competência para, entre outras atividades:

- (i) Implementar os controles de gestão de Riscos definidos pelo Conselho de Administração;
- (ii) Estabelecer procedimentos de gerenciamento de Riscos, coordenando e definindo padrões a serem seguidos quanto a ferramentas, metodologias, sistemas e formas de suporte;
- (iii) Fornecer apoio metodológico a Proprietários dos Riscos e responsáveis pelos processos da Companhia, por meio de ferramentas e serviços sob demanda, liderando e direcionando os esforços e objetivos com as diversas áreas da Companhia;
- (iv) Monitorar continuamente o sistema de gestão de Riscos, reportando as atividades de gestão de Riscos ao Conselho de Administração por meio do Comitê de Auditoria, e buscando melhorias para processos de gestão de Riscos e controles internos;
- (v) Atualizar a Matriz de Riscos sempre que ocorrer a revisão do plano estratégico, ou quando do surgimento de novos fatores de Risco;
- (vi) Auxiliar o Conselho de Administração, o Comitê de Auditoria e a Diretoria na análise qualitativa e quantitativa de Riscos corporativos;
- (vii) Elaborar relatórios de reporte ao Comitê de Auditoria e ao Conselho de Administração, consolidando a avaliação de Riscos da Companhia;

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|    | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>8/16                         | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

- (viii) Zelar pela aplicação e elaborar o plano de implantação para procedimentos e diretrizes do Código de Conduta Ética, bem como das demais políticas de integridade e controles internos, mitigando Riscos de conformidade e regulatórios;
- (ix) Encaminhar ao Comitê de Auditoria, para recebimento e tratamento, todas as denúncias de potencial descumprimento de dispositivos legais, regulamentos ou normativos internos, reportadas ao Canal Íntegro da Companhia ou identificadas por qualquer meio;
- (x) Acompanhar a implementação de ações de respostas e planos de ação;
- (xi) Desenvolver normas, políticas e procedimentos a fim de mitigar riscos e impactos relacionados a controles internos em todas as áreas da Companhia;
- (xii) Monitorar e mapear os processos e procedimentos relacionados a controles internos;
- (xiii) Atualizar os processos e procedimentos relacionados a controles internos; e
- (xiv) Reportar-se ao Comitê de Auditoria da Companhia quanto a questões estratégicas relacionadas a controles internos.

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|    | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>9/16                         | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

No que diz respeito a Compliance e integridade corporativa, a Área de Compliance, Gerenciamento de Riscos e Controles Internos tem competência para, entre outras atividades:

- (i) Tomar as medidas necessárias para garantir a aplicação e divulgação do Código de Conduta Ética da Companhia e, inclusive, fiscalizar e avaliar o seu cumprimento e eficácia;
- (ii) Propor novas normas ou políticas relacionadas ao programa de integridade da Companhia ou a revisão das já existentes;
- (iii) Orientar colaboradores frente a situações de conflito de interesse;
- (iv) Conduzir treinamentos periódicos acerca das condutas, princípios, conceitos e procedimentos previstos no Código de Conduta Ética, mantendo instrumentos adequados de controle de frequência, participação e retenção de informações;
- (v) Definir e acompanhar os procedimentos de contratação e monitoramento de parceiros;
- (vi) Receber e tratar as comunicações recebidas através do Canal Íntegro, sendo facultado o auxílio de outras áreas da Companhia (como Jurídico, Recursos Humanos, dentre outras) e/ou de assessores externos, conforme aplicável, garantindo a confidencialidade das informações e o anonimato do denunciante, se desejado, e práticas de não retaliação;
- (vii) Reportar-se ao Comitê de Auditoria quanto às suas atividades relacionadas à apuração de denúncias de violação às leis, regulamentos e normas internas da Companhia, encaminhando-lhe diretamente os casos mais graves;
- (viii) Decidir, com o auxílio de gestores e/ou de outras áreas da Companhia (como Jurídico, Recursos Humanos, dentre outras) e/ou de assessores externos, conforme aplicável, a respeito de sanções e medidas disciplinares aplicáveis, submetendo casos mais graves ao Comitê de Auditoria;
- (ix) Analisar a oferta e recebimento de brindes, cortesias, hospitalidade e ressarcimento de viagens, de modo que adiram aos termos do Código de Conduta Ética; e
- (x) Aprovar a realização de doações, patrocínios e eventos que atendam ao disposto no Código de Conduta Ética.

Compete aos Proprietários dos Riscos da Companhia:

- (i) Identificar os fatores de Riscos e os indicadores para a mensuração e monitoramento dos Riscos;
- (ii) Fornecer informações precisas, íntegras e suficientes para análises;
- (iii) Apresentar percepção quanto à exposição ao Risco sob sua responsabilidade, 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;

9

Aprovador(es):  
Conselho de Administração

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>10/16                | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>   |                           |                |                                |                                    |

- (v) Cumprir os Limites de Riscos aprovados pelo Conselho de Administração;
- (vi) 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
- (vii) Dar cumprimento às ações de respostas e ao plano de ação.

## 6. RISCOS AOS QUAIS A COMPANHIA ESTÁ EXPOSTA

A Companhia busca proteção para riscos divididos nas seguintes principais macro categorias, a serem consideradas e incluídas em seu Mapa de Riscos:

### Riscos Estratégicos

São aqueles associados à estratégia da Companhia na busca de criação, proteção e crescimento de valor – e incluem os Riscos concorrenciais, políticos e de imagem/reputacionais. Referem-se a decisões estratégicas na persecução de objetivos de negócios e/ou à capacidade ou habilidade para proteger-se ou adaptar-se a mudanças no ambiente externo – tais como político e econômico, de mercado, competidores, fusões e aquisições, disponibilidade de recursos, inovações e portfólio de produtos e/ou serviços.

### Riscos Operacionais

São aqueles que envolvem operação, sistemas, processos, controles internos, clientes, receitas e outros ativos ou atividades da Companhia que podem implicar perdas, danos e declínio quanto aos resultados da Companhia. Decorrem de inadequação, falha, deficiência ou fraude nos processos internos, que possam dificultar ou impedir a devida execução das atividades e/ou o alcance de objetivos. Dentre eles, podemos citar: inviabilidade do produto, não aderência do produto, clientes e mercado (baixo volume de vendas, perdas para concorrência, preço não condizente, produto não compatível, momento indevido de lançamento), dentre outros.

### 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 ou câmbio, na inflação, em financiamentos ou investimentos financeiros, entre outros. Dentre eles, podemos citar: perda financeira por cadastramento incorreto de índice de correção dos contratos, perda financeira devido a aplicações financeiras equivocadas, perdas financeiras decorrentes de ações ocasionadas por distratos, possibilidade de inadimplemento de obrigações financeiras, entre outros.

### Riscos de Conformidade e Regulatórios

São aqueles causados por eventual falha no cumprimento de leis, normas, regulamentos e políticas internas, ou pela existência de processos jurídicos em aberto ou futuros, que possam resultar em

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>11/16                | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

perda financeira e/ou prejudicar a imagem, a credibilidade e a reputação da Companhia. Dentre eles, podemos citar: atividades executadas em desacordo com políticas, normas e procedimentos da Companhia ou com a legislação e regulamentação aplicável, falhas no monitoramento da adesão à alteração/criação de leis e regulamentações, entre outros.

### Riscos Tecnológicos

São aqueles que podem ser causados pelo vazamento de dados/informações pessoais, roubo/vazamento de informações estratégicas (envio de arquivos confidenciais), acesso inadequado a ativos e recursos de TI, acesso remoto inseguro, dentre outros, que impactam na confidencialidade, integridade e disponibilidade das informações detidas pela Companhia.

### Riscos Socioambientais

São os riscos relacionados a questões ambientais e de direitos humanos, como a contaminação de água e solo, descarte indevido de resíduos sólidos e quaisquer outras questões socioambientais, como riscos de perdas decorrentes de efeitos negativos das atividades e operações da Companhia sobre a comunidade do entorno e a sociedade em geral.

## **7. DIRETRIZES**

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.

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.

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.

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 ou em processos; (ii) decisões estratégicas malsucedidas; ou (iii) falha na governança. Este entendimento visa a aperfeiçoar e fortalecer o modelo de governança corporativa da Companhia.

Todos os Riscos desenvolvidos, com limites aprovados, deverão ser refletidos no Mapa de Riscos e formalizados em relatórios, com planos de ação, se for o caso, incluindo designação de responsáveis e prazos de conclusão. Os relatórios deverão ser assinados pelo Proprietário do Risco e pelo Comitê de Auditoria.

A assunção de Riscos que possam comprometer a continuidade do negócio, e/ou a inobservância/extrapolação deliberada dos limites, no exercício de suas funções, estará sujeita às sanções previstas no Código de Conduta Ética Companhia.

|  |                           |                |                                       |                                    |
|--|---------------------------|----------------|---------------------------------------|------------------------------------|
|    | <b>POLÍTICA</b>           |                |                                       | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>12/16                       | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Setor:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |                                       |                                    |
| <b>Objetivo:</b> 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. |                           |                |                                       |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |                                       |                                    |

## 8. METODOLOGIA

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.

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 dos seguintes instrumentos:
- (i)** Entrevistas e reuniões com colaboradores chave da Companhia e Proprietários de Riscos;
  - (ii)** Monitoramento contínuo pela área de Compliance, Gerenciamento de Riscos e Controles Internos;
  - (iii)** Auditorias independentes nos processos internos da Companhia;
  - (iv)** Reportes e denúncias recebidos por meio do Canal Íntegro, disciplinado pelo Código de Conduta Ética.
- B. Avaliação:** cálculo do impacto e da probabilidade de ocorrência dos Riscos sobre os resultados projetados.
- (i) **Nível de Impacto:**** de acordo com a percepção e análise do avaliador quanto ao nível do provável impacto:

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>13/16                | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

| Categoria                          | Baixo  | Moderado   | Significativo  | Alto  |
|------------------------------------|--|--|--|---|
| <b>Estratégico</b>                 | Pequeno ajuste de rota sem mudança estratégica       | Pode afetar o marketshare mas sem prejudicar a posição             | Compromete o retorno esperado de um investimento                                     | Compromete relevantemente o resultado ou perda de posição de mercado                        |
| <b>Operacional</b>                 | Não trava o processo, mas infere morosidade no mesmo | Trava o processo mas há contorno                                   | Trava o processo e há possibilidade de contornar com análise                         | Trava o processo e não conhecimento de contorno. Precisa-se da contratação de especialistas |
| <b>Financeiro</b>                  | Não compromete as entradas e saídas de dinheiro      | Baixo compromete as entradas e saídas de dinheiro, mas há contorno | Compromete as entradas e saídas de dinheiro e exige interferência imediata de gestão | Compromete as entradas e saídas de dinheiro e não há contorno                               |
| <b>Conformidade e Regulatórios</b> | Possibilidade de Autuação                            | Pequena possibilidade de Condenação                                | Possibilidade real de Condenação   | Qualquer possibilidade de responsabilidade penal de sócios ou diretores ou Condenação Certa |
| <b>Tecnológicos</b>                | Compromete execução dos processos sem afetar prazos  | Compromete o cumprimento de prazos                                 | Compromete a qualidade do processo   | Compromete a entrega de produtos ou serviços dos processos                                  |
| <b>Socioambiental</b>              | Possibilidade de Autuação                            | Pequena possibilidade de Condenação                                | Possibilidade real de Condenação   | Qualquer possibilidade de responsabilidade penal de sócios ou diretores ou Condenação Certa |

Figura 2. Avaliação do Nível de Impacto do Risco

- (ii) **Probabilidade:** classificação de probabilidade deve ocorrer de acordo com a percepção e análise do avaliador quanto a ocorrência dos riscos:

| Probabilidade       | Descrição                                       |
|---------------------|---|
| <b>4 Muito Alta</b> | Esperado ocorrer na maioria das circunstâncias. |
| <b>3 Alta</b>       | Provavelmente ocorrerá.                         |
| <b>2 Média</b>      | Pode ocorrer no futuro.                         |
| <b>1 Baixa</b>      | Pode ocorrer, mas pouco provável.               |

Figura 3. Avaliação da Probabilidade do Risco

**C. Limite de Risco:** priorização e definição do Limite de cada Risco que a Companhia está disposta

13

Aprovador(es):  
Conselho de Administração

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>14/16                | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

a correr na busca pelo retorno e geração de valor, classificando os Riscos de acordo com as definições abaixo:

- (i) *Risco Alto*: representa ameaça potencial aos negócios da Companhia. Demanda ação gerencial prioritária para eliminar o componente de Risco ou ao menos reduzir sua severidade e/ou frequência.
- (ii) *Risco Significativo*: com alto impacto e baixa frequência, deve ser quantificado e monitorado regularmente para direcionar continuamente as estratégias de mitigação e/ou planos de contingência. O objetivo é o de estar preparado caso o evento venha a acontecer.
- (iii) *Risco Moderado*: de menor criticidade devido ao menor nível de impacto no valor dos negócios; foco deve ser o de definir níveis aceitáveis de perda por eventos e limites de competência que evitem que o nível de impacto se eleve ao longo do tempo.
- (iv) *Risco Baixo*: de menor criticidade, devido ao menor potencial e nível de impacto no valor dos negócios, podendo o custo do impacto ser menor do que o custo de mitigá-los; foco deve ser o de definir níveis aceitáveis de perda por eventos e limites de competência que evitem que o nível de impacto se eleve ao longo do tempo.

A definição do Limite do Risco consiste em classificar os resultados do cálculo de avaliação e analisar se os valores apresentados estão dentro do nível aceitável ou não – fornecendo, assim, base para que uma decisão sobre a implementação de tratamento, controles e ações de resposta seja efetuada. A Tabela abaixo fornece valores dos intervalos para comparação dos resultados e enquadramento:

|                   |  |
|-------------------|--|
| <b>Muito Alto</b> | Risco Inaceitável. Tratamento imprescindível deve ter alta prioridade. |
| <b>Alto</b>       | Risco Grave. Tratamento mandatório deve ter prioridade.                |
| <b>Médio</b>      | Risco Moderado. Tratamento recomendado.                                |
| <b>Baixo</b>      | Risco Aceitável. Tratamento opcional.                                  |

Figura 4. Classificação para Limite do Risco

Após as classificações em níveis e probabilidade e conforme os níveis das categorias, os riscos serão classificados conforme a Matriz de Riscos:

|   |                           |                |                                |                                    |
|---|---------------------------|----------------|--------------------------------|------------------------------------|
|   | <b>POLÍTICA</b>           |                |                                | Data da Revisão:<br>15/12/2021     |
|   | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>15/16                | Data de Implantação:<br>19/10/2021 |
| Título: Política de Gerenciamento de Riscos   |                           |                | Setor: Gerenciamento de Riscos |                                    |
| Aplicação: Corporativo  |                           |                |                                |                                    |
| Objetivo: 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. |                           |                |                                |                                    |
| As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.  |                           |                |                                |                                    |

|               |               |       |       |               |         |
|---------------|---------------|-------|-------|---------------|---------|
| IMPACTO       | Alto          | Médio | Alto  | Crítico       | Crítico |
|               | Significativo | Médio | Médio | Alto          | Crítico |
|               | Médio         | Baixo | Médio | Médio         | Alto    |
|               | Baixo         | Baixo | Baixo | Médio         | Médio   |
|               |               | Baixa | Média | Significativo | Alta    |
| PROBABILIDADE |               |       |       |               |         |

Figura 5. Modelo da Matriz de Riscos

- D. Tratamento:** a partir da identificação e avaliação dos Riscos, são implementadas ações de respostas, que consistem no tratamento e mitigação dos Riscos. As ações de respostas aos Riscos consideram os seguintes critérios:
- (i) **Rejeitar:** 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, como por meio de terceirização de operações e atividades;
  - (iii) **Mitigar:** reduzir a probabilidade e/ou impacto de um Risco para um Limite aceitável a Companhia;
  - (iv) **Aceitar/Reter:** nenhuma ação direta é tomada para alterar o nível de impacto ou a 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 ou contínuo).
- F. Monitoramento:** verificação periódica ou contínua da eficácia e adequação dos controles internos estabelecidos, em conjunto com a obtenção de informações que possam proporcionar melhorias no processo de gerenciamento de Riscos. Aplicável enquanto o Risco estiver tratado, respondido e/ou dentro do Limite de Riscos da Companhia, já que nesse caso nenhuma ação direta é tomada para alterar o nível de impacto ou probabilidade do Risco.

|  |                           |                |  |                                    |
|--|---------------------------|----------------|--|------------------------------------|
|    | <b>POLÍTICA</b>           |                |  | Data da Revisão:<br>15/12/2021     |
|  | Número:<br>POL-01-GRI-001 | Revisão:<br>01 | Folha:<br>16/16                        | Data de Implantação:<br>19/10/2021 |
| <b>Título:</b> Política de Gerenciamento de Riscos   |                           |                | <b>Sector:</b> Gerenciamento de Riscos |                                    |
| <b>Aplicação:</b> Corporativo  |                           |                |  |                                    |
| <b>Objetivo:</b> 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. |                           |                |  |                                    |
| <small>As informações contidas neste documento são de propriedade da Cantu Store e seu uso restrito aos destinatários autorizados. A reprodução total ou parcial deste documento não é permitida.</small>  |                           |                |  |                                    |

## 9. DISPOSIÇÕES GERAIS

No caso de conflito entre as disposições desta Política e do Estatuto Social, bem como em caso de lacuna de diretrizes na presente Política, 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.

Caso qualquer disposição desta Política venha a ser considerada inválida, ilegal ou ineficaz, essa invalidade será limitada à disposição em questão, na medida do possível – para que a validade, legalidade e eficácia das disposições remanescentes desta Política não sejam afetadas ou prejudicadas.

As violações dos termos da presente Política serão examinadas pela Área de Compliance, Gerenciamento de Riscos e Controles Internos, que as reportará ao Comitê de Auditoria, e tomará as medidas cabíveis, também sob a supervisão do Comitê de Auditoria – alertando, ainda, que certas condutas poderão constituir infração à legislação aplicável, sujeitando os responsáveis às penas previstas na legislação vigente.

Esta Política pode ser consultada em [www.ri.cantustore.com.br](http://www.ri.cantustore.com.br) e entra em vigor na data de sua aprovação pelo Conselho de Administração da Companhia – somente estando sujeita a modificações por deliberações do mesmo órgão.

## 10. DOCUMENTOS COMPLEMENTARES

- Enterprise Risk Management - Integrated Framework (COSO – Comitê das Organizações Patrocinadoras);
- DAD-01-CPL-001 - Código de Conduta Ética.

\* \* \*