

POLÍTICA DE GERENCIAMENTO DE RISCOS DA WESTWING COMÉRCIO VAREJISTA S.A.

INTRODUÇÃO

As atividades da Westwing Comércio Varejista S.A. e de todas as suas subsidiárias diretas e indiretas (“**Companhia**”) compreendem primordialmente: (i) o comércio varejista de móveis e artigos domésticos em geral, (ii) os serviços de montagem relacionados à atividade acima, (iii) o comércio varejista de alimentos e bebidas, (iv) o comércio varejista de cosméticos, produtos de perfumaria e de higiene pessoal, (v) o comércio varejista de artigos de vestuário e acessórios, (vi) o comércio varejista de eletrodomésticos, (vii) o comércio varejista de eletroeletrônicos, (viii) o comércio varejista de livros e revistas, (ix) o comércio varejista de cama, mesa e banho, (x) o comércio varejista de artigos de tapeçaria, tapetes, carpetes, persianas e outros, (xi) a importação, a exportação e o comércio varejista de produtos de uso doméstico e pessoal, artigos para decoração e outros, (xii) a intermediação, a representação, o agenciamento, a corretagem de serviços e de negócios em geral, inclusive o agenciamento de publicidades e de propagandas, (xiii) o comércio atacadista de artigos de cama, mesa e banho, (xiv) o comércio atacadista de lustres, luminárias e abajures, (xv) o comércio atacadista de artigos de tapeçaria, persianas e cortinas, (xvi) o comércio atacadista de móveis e artigos de colchoaria, (xvii) o comércio de produtos em lojas de variedade na internet, (xviii) as atividades de design de interiores, (xiv) a realização de serviços de arquitetura, (xv) as atividades de produção e edição de vídeos para divulgação na internet, (xvi) as atividades de representação comercial, (xvii) o comércio varejista de calçados em geral, e (xviii) administração de cartões de crédito. A Companhia reconhece que suas operações acarretam determinados riscos, cuja gestão é feita por diferentes departamentos em níveis de prevenção, identificação e correção, obedecendo a diversas estratégias de negócios e políticas internas aprovadas pela alta administração da Companhia.

Esta política de gerenciamento de riscos da Companhia (“**Política**”) descreve a forma por meio da qual a Companhia identifica, avalia, monitora e gerencia os riscos aos quais a Companhia está sujeita.

1 Objetivos

- 1.1** A presente Política foi desenvolvida tendo em vista as recomendações do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) e tem como principais objetivos estabelecer diretrizes e responsabilidades na gestão de riscos da Companhia no que diz respeito à identificação e análise dos riscos e assegurar a isenção das atividades e dos reportes de cada uma das áreas no desempenho de suas funções.
- 1.2** Esta Política estabelece os princípios e parâmetros a serem observados com relação ao processo de gerenciamento de risco da Companhia com vistas a identificar, avaliar, priorizar e gerenciar Riscos (conforme abaixo definido).
- 1.3** Esta Política também descreve o processo de gerenciamento de risco, os procedimentos de comunicação e as responsabilidades dos principais órgãos societários da Companhia.

2 Abrangência

2.1 Esta Política vincula todos os departamentos e empregados da Companhia. As subsidiárias da Companhia também deverão cumprir as disposições ora previstas.

3 Referências

3.1 Os seguintes documentos devem ser levados em consideração para a aplicação e interpretação dos termos desta Política:

- (i) COSO – ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*;
- (ii) O Código de Conduta;
- (iii) A Política de Divulgação de Informações da Companhia;
- (iv) A Política de Negociação de Valores Mobiliários da Companhia; e
- (v) A Política de Transações entre Partes Relacionadas da Companhia.

4 Definições

“Apetite para o Risco”

significa o nível de risco associado à consecução dos objetivos da Companhia. Periodicamente, o Comitê de Auditoria avalia e revisa o nível de risco aceitável assumido pela Companhia como um todo, para assegurar que o equilíbrio entre risco e benefício seja adequadamente gerenciado e alinhado. O Comitê de Auditoria reportará tais avaliações e níveis de risco periodicamente ao Conselho de Administração.

“Avaliação do Risco”

significa a avaliação quantitativa ou qualitativa da natureza e da magnitude do risco relativos aos objetivos da Companhia. A avaliação baseia-se em vulnerabilidades e ameaças conhecidas ou contingentes, assim como na probabilidade de concretização das ameaças e no potencial impacto sobre a Companhia.

“Gerenciamento do Risco”

significa o processo de avaliação e resposta ao risco relacionado aos negócios da Companhia com vistas a reduzir tais riscos a níveis aceitáveis. O gerenciamento do risco é parte do processo de avaliação e utiliza os resultados oriundos de tal processo para tomar decisões sobre a aceitação de riscos ou a tomada de medidas para reduzi-los.

“Risco”

significa a incerteza relacionada a certos eventos e seu potencial resultado que possa ter um efeito significativo sobre as atividades da Companhia. Todas as atividades da Companhia podem representar algum risco decorrente de potenciais ameaças ou da não concretização de

oportunidades, que podem prejudicar, impedir, afetar ou interferir na consecução dos objetivos sociais.

“Risco Estratégico”

significa o risco de implementação de uma estratégia errada, inadequada ou ineficaz que deixe de atingir os objetivos da Companhia.

“Risco Operacional”

significa o risco de prejuízo devido a falhas, deficiências ou inadequação de processos, pessoal e sistemas internos de suporte às atividades da Companhia ou, ainda, eventos externos, incluindo, mas não se limitando, risco de *compliance* associado à inadequação ou deficiência em contratos, assim como sanções devidas ao não cumprimento de leis e regulamentos e indenizações de danos causados a terceiros resultantes das atividades da Companhia. Também inclui fraudes internas e externas.

“Risco de Imagem”

significa o risco de prejuízo decorrente da exposição negativa da marca em redes sociais, por meio de reclamações, mensagens e comentários divulgados pelos clientes.

“Risco de Infraestrutura de Sistema de Tecnologia da Informação”

Significa o risco de falhas nos serviços de infraestrutura de tecnologia da informação, incluindo anomalias nos indicadores de serviços, servidores, bancos de dados e *endpoints* de terceiros, bem como lentidões e oscilações na plataforma, que podem acarretar a redução ou interrupção total ou parcial das atividades.

“Risco de Vendas”

Significa o risco de oscilações nos níveis de transações realizadas na plataforma e lojas físicas da Companhia, que podem estar limitados a um segmento específico ou envolver as vendas de uma maneira geral. Os Riscos de Vendas podem decorrer de uma deficiência na estratégia ou incentivos de *marketing*, em problemas envolvendo determinado grupo de produtos, em instabilidades e falhas verificadas nos sistemas de meio de pagamento, no carregamento do checkout (hipótese em que tratar-se-á também de um Risco de Infraestrutura de Sistema de Tecnologia da Informação), bem como falhas em abastecimento de mercadorias na plataforma e transporte.

- “Risco de Liquidez”** significa o risco de falta de capacidade financeira da Companhia, ou a sua falta de capacidade de se financiar para pagar suas dívidas previstas e imprevistas, efetivas e futuras, incluindo operações com garantias, sem afetar suas operações do dia a dia e sem incorrer em perdas significativas.
- “Risco de Compliance”** significa o risco de estar sujeito a quaisquer sanções legais de cunho reputacional ou regulatórias, ou prejuízo financeiro que a Companhia possa sofrer em decorrência de sua falha em cumprir as leis e regulamentos aplicáveis, políticas internas, códigos de conduta e padrões de boas práticas.
- “Risco de Informação”** significa o risco relacionado à perda, ao mau uso ou à divulgação não autorizada de dados pessoais sensíveis ou informações confidenciais de clientes, fornecedores, parceiros de negócios, acionistas internos ou externos que possam causar danos ou transtornos a qualquer indivíduo, ameaçar os negócios da Companhia ou prejudicar sua reputação.
- “Risco Estrutural do Meio de Pagamento”** significa o risco relacionado à interrupção estrutural das operações desenvolvidas pelas empresas de meio de pagamento que prestam serviços para a Companhia, o que pode vir a prejudicar o fluxo de pagamento relacionado às atividades da Companhia. O Risco Estrutural do Meio de Pagamento é mitigado em razão do fato de a Companhia contar com mais de um meio de pagamento em funcionamento, podendo direcionar as transações de um sistema para o outro.

5 Processo de Gerenciamento de Riscos

- 5.1** O gerenciamento do risco é um elemento crucial das estratégias da Companhia, já que fornece um processo sistemático para identificar riscos relacionados às atividades da Companhia bem como ao mercado de atuação da Companhia. Tal processo envolve a categorização e a avaliação de cada risco e a aplicação de controles gerenciais para mitigar o risco, baseados em um julgamento acerca do impacto provável caso nenhuma medida seja tomada, combinado com uma avaliação da probabilidade de nova ocorrência do risco.
- 5.2** Com base no *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework* (COSO), a Companhia estabelece um processo de gerenciamento dos riscos que engloba os seguintes componentes:
- (i) **ambiente interno** – envolve o estabelecimento da base de como riscos e controles são visualizados e tratados pelos empregados da Companhia;

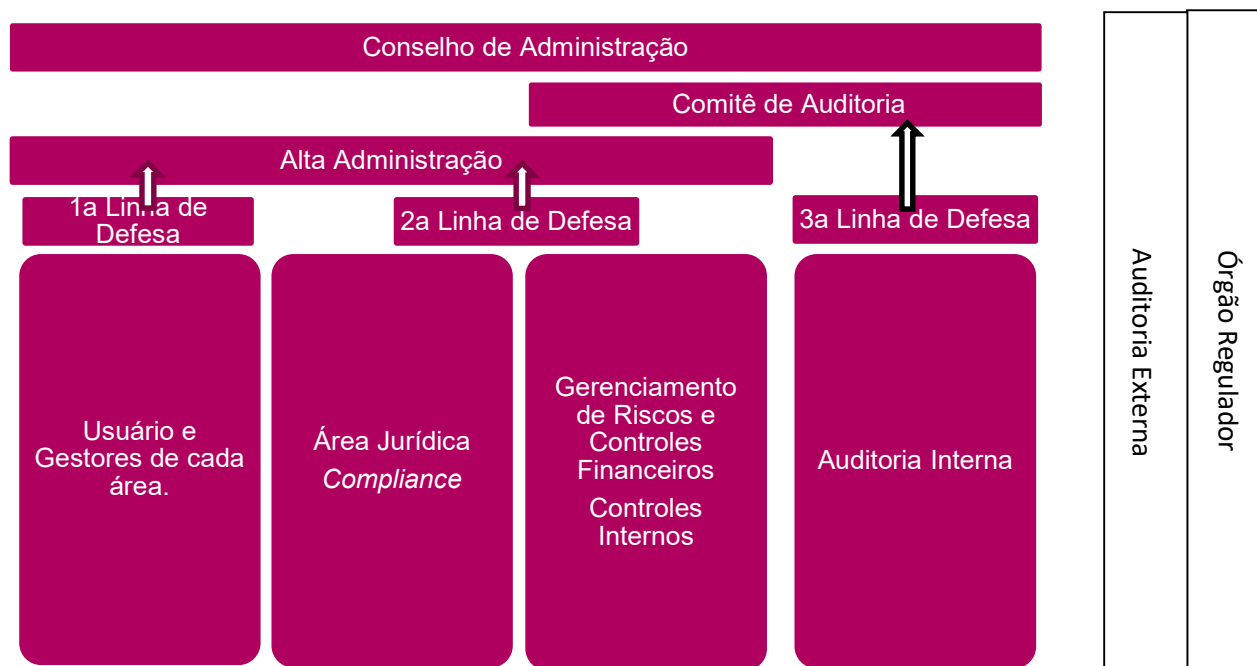
- (ii) **fixação de objetivos** – pressupõe a certificação de que a administração dispõe de um processo para fixar objetivos e que os objetivos escolhidos se alinham à missão e aos princípios da Companhia;
- (iii) **identificação de eventos** - inclui a identificação de fatores internos e externos que possam afetar adversamente as estratégias de negócios e as metas da Companhia;
- (iv) **avaliação do risco** – exige uma análise dos riscos identificados para formar uma base para determinar como deverão ser gerenciados;
- (v) **resposta ao risco** – exige que a administração implemente um conjunto de iniciativas e planos de ação para mitigar riscos quando for o caso, com base no perfil de risco na Companhia;
- (vi) **atividades de controle** – inclui o estabelecimento e a execução de políticas e procedimentos para auxiliar a garantir que a estrutura selecionada de resposta ao risco é adequada e a gestão dos mesmos seja efetivamente realizada;
- (vii) **informação e comunicação** – exige que as informações relevantes sejam identificadas, capturadas e comunicadas em formato e prazo que permitam às pessoas desempenhar suas atribuições; e
- (viii) **monitoramento** – exige revisão e atualização permanentes do processo de gestão de riscos da Companhia para garantir que esta esteja apta a reagir prontamente a circunstâncias diferentes e inesperadas.

5.3 A Companhia garantirá que haja suficiente flexibilidade para reagir rapidamente e para mitigar adequadamente os Riscos. A Companhia reconhece que os Riscos podem ser efetivamente gerenciados se essa gestão estiver incutida na cultura da Companhia.

5.4 O processo de gerenciamento do risco será realizado por meio de auditoria interna e externa visando a minimizar as consequências da ocorrência de um risco com base em impacto e probabilidade, reconhecendo-se que o risco propriamente dito pode não ser eliminado.

6 Estrutura de Detecção e Prevenção de Riscos em Três Linhas de Defesa

A Companhia adota uma estrutura de detecção e prevenção de riscos composta por três linhas de defesa, conforme figura abaixo, que mostra como se dá a comunicação pelo plano hierárquico da Companhia.



- 6.1** A primeira linha de defesa é composta pelos colaboradores e gestores de cada área, sendo que o colaborador é o responsável por detectar quaisquer riscos no dia-a-dia de suas atribuições e informá-lo para os seus gestores, que deverão avaliar o risco e ponderar eventuais medidas cabíveis.
- 6.2** A segunda linha de defesa é composta por áreas da companhia que não acumulam atividades operacionais no desempenho de suas funções, tais como controles internos e gerenciamento de riscos, além do Departamento Jurídico e de *Compliance*. Tais departamentos são supervisionados pela Alta Administração e, no âmbito da gestão de risco e de conformidade, pelo Comitê de Auditoria. Essas funções são implementadas para garantir que os controles e os processos de gerenciamento de riscos executados pela primeira linha de defesa estejam funcionando de acordo com os procedimentos, normas, políticas e legislações pertinentes, bem como auditar se as recomendações oriundas de Relatório de Auditoria realizados foram considerados nos planos de ação.
- 6.3** A terceira linha de defesa é desempenhada pela área de Auditoria Interna, pois são estes os responsáveis por fornecer ao órgão de governança e à alta administração da Companhia as avaliações objetivas e abrangentes, com o maior nível de independência dentro da organização. É a Auditoria Interna que realiza as avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linha de defesa alcançam os objetivos em relação ao gerenciamento de riscos e controles.

7 Responsabilidades

7.1 Conselho de Administração

O Conselho de Administração da Companhia será responsável por:

- (i) determinar o Apetite por Riscos e estabelecer a cultura da gestão do risco dentro da Companhia, especialmente com relação a novas iniciativas e riscos emergentes;
- (ii) tomar as decisões principais com relação ao processo de gestão de riscos da Companhia, incluindo os que possam afetar o perfil de risco ou exposição da Companhia;
- (iii) avaliar a efetividade do sistema de controles internos, com o assessoramento do Comitê de Auditoria;
- (iv) aprovar quaisquer mudanças nesta Política; e
- (v) revisar, monitorar e aprovar as estratégias gerais da Companhia para a gestão do risco e os papéis e relatórios elaborados pelo Comitê de Auditoria e pelas divisões de controles internos e *compliance*.

7.2 Diretoria

A Diretoria da Companhia será responsável por:

- (i) implementar as estratégias da Companhia aprovadas pelo Conselho de Administração com relação à Gestão do Risco;
- (ii) propor ao Conselho de Administração o Apetite por Risco da Companhia;
- (iii) conduzir uma revisão periódica desta Política e apresentar quaisquer sugestões ao Conselho de Administração;
- (iv) avaliar periodicamente a Avaliação de Risco, relatando quaisquer descobertas ao Conselho de Administração;
- (v) avaliar e monitorar o Risco Estratégico;
- (vi) identificar quaisquer Riscos antecipadamente e conduzir o Gerenciamento de Risco correlata; e
- (vii) auxiliar na elaboração dos relatórios relacionados ao Gerenciamento do Risco.

7.3 Comitê de Auditoria

O Comitê de Auditoria da Companhia, órgão de assessoramento do Conselho de Administração, com autonomia operacional, estará encarregado de:

- (i) rever o cumprimento pela Companhia das leis, padrões e regulamentos aplicáveis;
 - (ii) avaliar e analisar o uso e a confiabilidade dos controles internos, riscos de *compliance* e corporativos;
 - (iii) monitorar as exposições de Risco da Companhia;
 - (iv) fiscalizar o desempenho de terceiros contratados para dar suporte ao staff designado para desempenhar funções de *compliance*, controles internos e risco corporativo;
-

- (v) revisar as principais políticas da Companhia, incluindo as políticas internas e o Código de Conduta Ética, propondo quaisquer mudanças ao Conselho de Administração;
- (vi) coordenar e monitorar as atividades de canal de denúncias (*whistleblower*) e ouvidoria (*ombudsman*), assegurando a autonomia, sigilo, confidencialidade e um ambiente livre de retaliações;
- (vii) avaliar e monitorar o Risco de Crédito e o Risco de Liquidez;
- (viii) investigar e monitorar eventos que possam prejudicar os controles internos e a política de *compliance* da Companhia; e
- (ix) fornecer treinamento recorrente ao pessoal da Companhia com vistas a assegurar que sejam capazes de identificar, evitar, avaliar, monitorar e mitigar Riscos.

7.4 Áreas Jurídica e de Compliance

As áreas Jurídica e de *Compliance* se reportam ao Conselho de Administração e, dentre outras competências previstas nas normas internas da Companhia, estarão encarregadas de:

- (i) avaliar e monitorar o Risco de *Compliance*;
- (ii) monitorar o cumprimento e auxiliar na interpretação de normativos emanados pelos órgãos reguladores a que a Companhia esteja sujeita;
- (iii) preparar boletins informativos e encaminhar para as áreas de interesse, quando julgar conveniente;
- (iv) mapear e conduzir treinamentos de *compliance* às áreas de interesse, os quais poderão envolver questões atinentes à legislação trabalhista, tributária, societária, de proteção de dados pessoais, entre outras;
- (v) auxiliar a área de ouvidoria na apuração e análise das medidas disciplinares a serem aplicadas em decorrência de violação do Código de Ética e Conduta da Companhia; e
- (vi) reportar bimestralmente à Área de Riscos, Controles Internos e Auditoria Interna na avaliação e o Gerenciamento de Riscos de Compliance.

7.5 Área de Riscos e Controles Internos

Os colaboradores da Companhia designados para desempenhar funções de controles internos e riscos corporativos se reportam à Alta Administração e estarão encarregados de:

- (i) estabelecer o processo de gestão do risco da Companhia;
 - (ii) coordenar e determinar as diretrizes a serem seguidas no tocante aos procedimentos de controles internos e risco corporativo;
 - (iii) avaliar e monitorar o Risco de *Compliance*, o Risco Operacional e o Risco de Informação;
-

- (iv) realizar no mínimo uma revisão anual do sistema de controles internos da Companhia; e
- (v) coordenar a força de trabalho interna destinada a detectar quaisquer Riscos e monitorar a eficácia do processo de Gerenciamento do Risco.

7.6 Área de Auditoria Interna

A área de Auditoria Interna responde diretamente ao Comitê de Auditoria, se reporta ao Conselho de Administração através do Comitê de Auditoria e é responsável por:

- (i) monitorar, avaliar e realizar recomendações visando a aperfeiçoar os controles internos e as normas e procedimentos estabelecidos pelos administradores;
- (ii) fornecer ao conselho de administração, ao comitê de auditoria e à administração avaliações abrangentes baseadas no maior nível de independência e objetividade dentro da organização;
- (iii) preparar relatórios bimestrais que descrevam os Riscos da Companhia e a avaliação de Risco correlata, e submetê-los ao Comitê de Auditoria;
- (iv) prover avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle;
- (v) avaliar a eficácia, suficiência e aplicação dos controles contábeis, financeiros e operacionais;
- (vi) determinar a extensão do cumprimento das normas, dos planos e procedimentos vigentes;
- (vii) determinar a extensão dos controles sobre a existência dos ativos da empresa e da sua proteção contra todo tipo de perda;
- (viii) determinar o grau de confiança, das informações e dados contábeis e de outra natureza, preparados dentro da empresa;
- (ix) avaliar a qualidade alcançada na execução de tarefas determinadas para o cumprimento das respectivas responsabilidades;
- (x) avaliar os riscos estratégicos e de negócio da organização.