

POLÍTICA DE GESTÃO DE RISCOS
br MALLS PARTICIPAÇÕES S.A.

CNPJ/MF Nº 06.977.745/0001-91
NIRE Nº 33.3.0028170-3

COMPANHIA ABERTA
(BRML3)

CAPÍTULO I
DEFINIÇÕES

1.1. Os termos e expressões listados a seguir, quando utilizados nesta Política, terão o seguinte significado:

- (a) “**Apetite ao Risco**” significa nível máximo ao qual a Empresa está disposta a se expor em relação ao(s) risco(s) para cumprir seus objetivos estratégicos e agregar valor aos stakeholders.
- (b) “**Compliance (ou conformidade)**” significa cumprimento de regulamentações, leis (fiscais, tributárias, trabalhistas, ambientais etc.), covenants, contratos e normas, procedimentos, diretrizes e políticas internas que se aplicam ao negócio.
- (c) “**Consequência de Risco**” tem o significado resultado da efetiva concretização do risco.
- (d) “**Committee of Sponsoring Organizations of the Treadway Commission (COSO)/Comitê das Organizações Patrocinadoras – ERM**” significa instituição privada, sem fins lucrativos, que visa a proporcionar documentos e/ou relatórios financeiros com o maior nível de veracidade possível, utilizando, para isto, princípios como ética empresarial, transparência, controles internos, gerenciamento de riscos e governança corporativa. Este Comitê estabeleceu uma metodologia de Gestão de Riscos que é referência no mercado, denominada Enterprise Risk Management (ERM) ou Gestão de Riscos Empresariais.
- (e) “**Dono do Risco**” significa colaborador indicado pela Empresa para criar e implementar plano de ação para mitigar o risco que está sob sua tutela.
- (f) “**Fator de Risco**” significa qualquer condição que possa ampliar a probabilidade de ocorrência do risco.

- (g) **“Gestão de Riscos”** significa de acordo com o COSO ERM, o gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.
- (h) **“Grupo Executivo de Riscos”** significa grupo de pessoas indicadas, cuja função é auxiliar no processo de Gestão de Riscos, apoiando os colaboradores instituídos como Donos dos Riscos e a Administração.
- (i) **“Impacto do Risco”** significa avaliação qualitativa e/ou quantitativa do efeito dos riscos nos objetivos estratégicos da Empresa.
- (j) **“Indicador de Risco - Key Risk Indicator (KRI)”** significa métrica utilizada para avaliar, com base em análises dos ambientes interno e externo da Empresa, o nível dos riscos identificados em um processo.
- (k) **“Matriz de Risco”** significa representação gráfica de exposição do impacto versus probabilidade dos riscos identificados pela Empresa.
- (l) **“Plano de Resposta aos Riscos”** significa conjunto de medidas adotadas para diminuir o risco inerente a um nível que esteja em consonância com o apetite a risco da Empresa.
- (m) **“Risco”** significa incerteza sobre a possibilidade de ganhos ou perdas, no momento de ocorrência de acontecimentos relacionados aos seus objetivos.
- (n) **“Risco Bruto (ou Inerente)”** significa risco que terá de ser enfrentado caso não seja possível atuar de modo que altere a probabilidade e/ou o impacto dos acontecimentos relacionados à Empresa.
- (o) **“Risco Residual”** significa risco que se mantém após a adoção de iniciativas e esforços para proporcionar respostas aos riscos identificados na Empresa.
- (p) **“Riscos Estratégicos”** significa riscos que advêm da falta de capacidade em se resguardar de eventos desfavoráveis ao cumprimento de suas estratégias.
- (q) **“Riscos Operacionais”** significa riscos que se relacionam com todo o ambiente interno, por meio de equívocos humanos e/ou de sistemas ou devido à ausência de treinamentos aos colaboradores.

- (r) **“Stakeholders (Parte Interessada)”** significa agentes que influenciam ou sofrem influência da Empresa.
- (s) **“Tolerância a Risco”** significa, de acordo com o COSO ERM, o nível de variação aceitável quanto à realização de um determinado objetivo.

CAPÍTULO II PROPÓSITO E ABRANGÊNCIA

- 2.1. A presente Política tem por objetivo definir diretrizes para Gestão de Riscos e possibilitar a identificação, avaliação, priorização, tratamento, comunicação e o monitoramento dos riscos da brMalls. A política objetiva, também, difundir padrão de linguagem de Gestão de Riscos, de maneira que fortaleça e estimule sua cultura.
- 2.2. Esta Política aplica-se aos negócios da brMalls, empresas controladas e administradas.

CAPÍTULO III RESPONSABILIDADES

- 3.1. Conselho de Administração:
 - i. Aprovar a Política de Gestão de Riscos;
 - ii. Aprovar os membros do Grupo Executivo de Riscos;
 - iii. Aprovar o grau de apetite a risco aceitável;
 - iv. Aprovar os riscos priorizados;
 - v. Aprovar plano de resposta dado aos riscos priorizados; e
 - vi. Acompanhar os resultados do processo de gerenciamento dos riscos.
- 3.2. Comitê de Auditoria:
 - i. Recomendar a política de gestão de riscos ao Conselho de Administração;
 - ii. Colaborar na discussão sobre o grau de apetite a risco;
 - iii. Compreender, avaliar e acompanhar o mapa de riscos;
 - iv. Acompanhar o andamento das atividades do Grupo Executivo de Riscos; e

- v. Acompanhar as mudanças na avaliação de criticidade dos riscos.

33. Grupo Executivo de Riscos:

- i. Propor o processo e mecanismos para a Gestão de Riscos da Empresa;
- ii. Propor o planejamento de trabalho em gestão de riscos;
- iii. Avaliar o mapa de riscos e as respostas dos riscos;
- iv. Acompanhar e avaliar o andamento das ações para a mitigação dos riscos (planos de ação);
- v. Reportar o status das ações para a mitigação dos riscos ao Comitê de Auditoria e ao Conselho de Administração;
- vi. Entender a metodologia de cálculo do apetite a risco;
- vii. Propor e monitorar o apetite a risco da Empresa;
- viii. Acompanhar e reportar as mudanças na avaliação de criticidade dos riscos; e
- ix. Deliberar sobre a definição dos Donos dos Riscos.

34. Estrutura de Gestão de Riscos:

- i. Ser a guardiã e difundir a política, processo e mecanismos de gerenciamento de riscos do grupo brMalls;
- ii. Auxiliar no desenvolvimento do gerenciamento de riscos, da política e manual;
- iii. Propor e manter atualizados a Política e o Manual de Gestão de Riscos, assim como padrões e mecanismos de reporte próprios de informações;
- iv. Entender a metodologia do cálculo do apetite a risco, calcular e atualizar o valor do apetite a risco periodicamente ou quando da ocorrência de eventos relevantes;
- v. Coordenar e monitorar o processo de identificação e avaliação dos riscos da Empresa;
- vi. Promover treinamentos de Gestão de Riscos aos colaboradores, buscando disseminar uma cultura de Gestão de Riscos;
- vii. Assessorar e monitorar as ações para a mitigação dos riscos (planos de ação);
- viii. Assessorar o Dono do Risco na criação de indicadores de riscos;

- ix. Manter o mapa dos riscos atualizados e reportar o mapa de riscos ao Grupo Executivo de Riscos; e
- x. Elaborar e revisar a Régua de Probabilidade e Impacto.

35. Donos dos Riscos:

- i. Comunicar à área de Gestão de Riscos eventuais mudanças significativas na probabilidade e no impacto ou qualquer outra característica do risco;
- ii. Efetuar revisão técnica do risco, do fator deste risco, das respostas e da avaliação do risco e elaborar a ficha de riscos;
- iii. Implantar ações necessárias, inclusive com o envolvimento de outras áreas, alinhadas ao plano de resposta deliberado pelo Conselho de Administração para a mitigação dos riscos;
- iv. Desenvolver indicadores e níveis de exposição dos riscos e acompanhar os resultados ao risco sob sua responsabilidade;
- v. Efetuar reportes periódicos ao Grupo Executivo de Gestão de Riscos e o Grupo Executivo de Riscos sobre o desenvolvimento de ações para a mitigação dos riscos; e
- vi. Realizar a avaliação do risco em relação à sua probabilidade e ao seu impacto.

CAPÍTULO IV

PRINCÍPIOS DA GESTÃO DE RISCOS

Gestão de Riscos está diretamente relacionada ao crescimento rentável e perene do Grupo brMalls, gerando valor e proteção para seus acionistas, uma vez que permite a identificação de ameaças, oportunidades de negócio, além da tomada de decisões melhor embasadas em função do conhecimento dos riscos que ameaçam o alcance de seus objetivos estratégicos. De acordo com as orientações do COSO ERM, a gestão de riscos deve ocorrer dentro das quatro categorias de objetivos empresariais, sendo estes objetivos: estratégicos, operacionais, de comunicação e de conformidade.

O Gerenciamento de Riscos tem como finalidade reduzir a materialização de eventos

que impactem negativamente os objetivos estratégicos, corporativos e de negócios, por meio da excelência no gerenciamento de riscos. A Gestão de Riscos, por meio de um enfoque estruturado e da melhor compreensão das inter-relações entre riscos, alinha a estratégia, os processos, as pessoas, a tecnologia e os conhecimentos, aproveitando os benefícios inerentes à diversificação, objetivando a preservação e a criação de valor para a Empresa e para os seus acionistas. O processo de gerenciamento de riscos deve contemplar, ao menos, etapas de identificação, mensuração, avaliação, definição de tratativas e monitoramento dos riscos. As definições e atividades relacionadas com cada uma das etapas e subetapas do processo são detalhadas no Manual de Gestão de Riscos.

CAPÍTULO V

DIRETRIZES DA GESTÃO DE RISCOS

- A Gestão de Riscos deve estar alinhada com o planejamento estratégico da brMalls;
- A Gestão de Riscos é contínua e o portfólio de riscos deve ser atualizado anualmente e/ou na ocorrência de eventos internos ou externos que afetem os objetivos estratégicos da brMalls;
- Todos os profissionais envolvidos no processo de gerenciamento de riscos devem ser treinados de forma adequada e tempestiva para o cumprimento de suas atribuições;
- A Gestão de Riscos deve fazer parte da cultura do Grupo brMalls, sendo presente em todos os processos e atividades;
- A liderança deve disseminar uma cultura de Gestão de Riscos entre profissionais de todos os níveis organizacionais e nas suas respectivas áreas de atuação, visando a aplicação dos princípios e a aderência aos procedimentos de Gestão de Riscos;
- A tomada de decisões embasada em riscos deve se tornar parte da gestão da companhia, objetivando a preservação e a criação de valor;
- Oferecer de forma adequada aos acionistas o acesso à informação clara e objetiva sobre os principais riscos e como estes são gerenciados de forma conservadora e

tempestiva;

- Aplicar e reconhecer uma metodologia formal, uma linguagem adequada ao público alvo e um padrão de normativos (políticas e procedimento internos) orientados pelas boas práticas de mercado, com o propósito não somente de permitir a melhor compreensão da Gestão de Riscos por todas as áreas, mas também de atender agentes externos e reguladores;
- A Gestão de Riscos deve ter interfaces com os processos de Compliance, Controles Internos e Auditoria Interna, unindo esforços para a identificação antecipada de riscos e a gestão conservadora e tempestiva;
- Os riscos identificados devem ser analisados e classificados de acordo com sua natureza, sua categoria e pela origem dos eventos (internos ou externos) e ter seu tratamento definido baseado nestas características. Se necessário, devem ser implementados planos de ação, através da definição de Donos dos Riscos e de planos de monitoramento;
- A decisão de tomada de risco deve ser feita pelas alçadas competentes previamente aprovadas, sendo os riscos de alçadas superiores ser partilhados com os profissionais chave. Eventuais descumprimentos das alçadas estabelecidas estão sujeitos à aplicação da Política de Gestão de Consequências;
- A Gestão de Riscos tenha independência, assim como segregação de funções entre os tomadores de riscos e os profissionais responsáveis pelo monitoramento destes; e
- A melhoria contínua do processo de Gestão de Riscos deve ser alcançada através do monitoramento contínuo, permitindo um gerenciamento dos riscos de forma adequada e o aperfeiçoamento do processo através de ciclos de avaliação e revisões frequentes.

CAPÍTULO VI

PROCESSO DE GERENCIAMENTO DE RISCOS

O processo de Gerenciamento de Riscos da brMalls prevê a participação de todos os órgãos da empresa envolvidos nos esforços de gerenciamento de riscos e visa

estabelecer premissas para equalizar suas estratégias e seus objetivos às metas de crescimento e de retorno de investimentos aos respectivos riscos e oportunidades.

Portanto essas premissas a serem utilizadas para mitigar a exposição da empresa aos riscos inerentes às suas operações compreendem as atividades para:

- i. Alinhar o apetite / tolerância aos riscos com a estratégia da brMalls;
- ii. Fortalecer as decisões em resposta aos riscos (evitar, reduzir, compartilhar e aceitar);
- iii. Reduzir as surpresas e prejuízos operacionais;
- iv. Identificar e administrar riscos múltiplos e entre empreendimentos e processos; e
- v. Aproveitar oportunidades e otimizar a alocação de capital.

Com base na estrutura de premissas estabelecida e o alinhamento dos objetivos nos níveis da organização, a estrutura de gerenciamento de riscos corporativos classificará os riscos em quatro categorias:

- Estratégicos – metas gerais, alinhadas com o que suportem à sua missão;
- Operações – utilização eficaz e eficiente dos recursos;
- Comunicação – confiabilidade de relatórios; e
- Regulatórios e conformidade – cumprimento de leis e regulamentos aplicáveis.

O Gerenciamento de Riscos terá como objetivo principal monitorar as atividades relacionadas a:

- i. Conformidade das operações às legislações aplicáveis;
- ii. Alinhamento dos processos e controles aos objetivos da brMalls;
- iii. Interrupção das atividades;
- iv. Fraudes internas e externas;
- v. Falhas na execução das atividades operacionais da empresa;
- vi. Confiabilidade das informações utilizadas durante a tomada de decisão;
- vii. Existência de passivos trabalhistas e segurança do trabalho;
- viii. Práticas inadequadas relativas a clientes, produtos e serviços;
- ix. Falhas em sistemas de tecnologia da informação;
- x. Adequada gestão de pessoas;
- xi. Ambientais, sociais e de sustentabilidade;
- xii. Financeiros, econômicos e de mercado; e
- xiii. Reputação e imagem.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

A Revisão poderá ocorrer anualmente ou sempre que houver alteração no processo e/ou responsabilidade de gerenciamento de risco, sendo certo que qualquer mudança deve ser aprovada pelo Grupo Executivo de Gestão de Risco.