

OBJETIVO

A presente Política de Gerenciamento de Riscos, aprovada em reunião do Conselho de Administração, em 18 de dezembro de 2024, tem por objetivo estabelecer os princípios, diretrizes e responsabilidades a serem observados no processo de Gestão de Riscos da Marisa Lojas S.A. e suas coligadas e/ou controladas (Marisa), de forma a possibilitar a adequada identificação, avaliação, direcionamento, monitoramento e comunicação dos riscos, visando a perpetuidade dos negócios.

1. APLICAÇÃO

Esta Política tem abrangência nacional, revoga e substitui a(s) política(s) interna(s) sobre o mesmo tema. Possui valor jurídico e envolve a responsabilidade dos membros da Alta Administração e de todos os colaboradores e/ou prestadores de serviços.

As responsabilidades sobre os riscos e controles internos são divididas entre as três linhas existentes na Companhia, com o objetivo de gestão apropriada:

1.1 Modelo das Três Linhas

As responsabilidades sobre os riscos e controles internos são divididas entre as três linhas existentes na Companhia, com o objetivo de gestão apropriada:

1ª Linha: é composta por todas as áreas de negócios e operacionais da Companhia, as quais são responsáveis por identificar e avaliar seus riscos, desenvolver e aplicar controles, monitorar continuamente o ambiente de riscos, reportar a materialização de eventos e estabelecer melhorias nos processos para gestão dos riscos, a exemplo da implementação de planos de ação. São, portanto, os responsáveis pela tomada de decisões quanto à gestão de riscos no dia a dia dos processos e atividades realizados na Companhia.

2ª Linha: é composta pelas áreas que possuem como responsabilidade realizar atividades de assessoria e suporte às demais áreas da Companhia no tocante à identificação e avaliação de riscos e controles, além de monitorar o ambiente de riscos e prover à Diretoria Executiva, ao Comitê de Auditoria e Riscos, o devido reporte e conclusões sobre as atividades realizadas.

Essas áreas fornecem supervisão e suporte sobre as atividades de gerenciamento de riscos às

áreas da 1ª Linha nos negócios, e auxilia na implementação de mecanismos eficazes de gerenciamento de riscos para mitigar os riscos. Dentre as áreas que compõem esta linha de defesa estão a Gestão de Riscos e Controles Internos.

3ª Linha: é composta pela Auditoria Interna, responsável pela revisão e avaliação independente dos processos e controles internos. Dessa forma, a função de 3ª Linha fornece garantia independente de que o negócio está efetivamente aplicando políticas e processos de gerenciamento de risco de acordo com as expectativas da Alta Administração da Companhia.

2. TERMOS E DEFINIÇÕES

“Marisa”: Utilizado para abreviar a razão social Marisa Lojas S.A. e quando esta abreviação for citada neste documento, entende-se que estão relacionadas as suas coligadas e/ou controladas e/ou companhias.

“Companhia”: Classificado com este nome a Marisa Lojas S.A. e suas coligadas e/ou controladas, ou seja, as empresas que fazem parte do conglomerado denominado MBank Marisa: a empresa M. Pagamentos S.A. Crédito, Financiamento e Investimento e a empresa M Cartões - Administradora De Cartões De Crédito Ltda.

“Colaborador”: Empregado, colaborador, estagiário, prestador de serviço, terceirizado, representante, conveniado, credenciado, fornecedor, menor aprendiz, que venham a ter relacionamento, direta ou indiretamente, com a Companhia.

“Risco”: possibilidade de ocorrência de evento(s), externo(s) ou interno(s), que possa(m) afetar negativamente a realização dos objetivos da Marisa ou de seus processos.

“Riscos Corporativos”: abrangem os principais eventos de riscos estratégicos, operacionais, financeiro, regulatório, mercado, liquidez, crédito, imagem / reputacional, e socioambiental, que impactam as atividades ou o atendimento aos objetivos da Companhia.

“Risco Inerente”: Risco intrínseco à atividade.

“Risco Residual”: Risco que se mantém após a adoção de iniciativas e esforços para redução / mitigação dos impactos ou probabilidade de materialização dos riscos inerentes da Companhia.

“Fator de Risco”: Condição que, individualmente ou combinada, possa ocasionar ou aumentar a probabilidade de materialização, ou o eventual impacto do risco.

“Dono do Risco”: Colaborador responsável por identificar, tratar e acompanhar o risco que está sob sua responsabilidade, conforme indicado pela Companhia.

“Ação Mitigatória”: ações tomadas visando minimizar a exposição ao risco, bem como reduzir o impacto e/ou a probabilidade de materialização dele.

“Impacto do Risco”: consequência/alcance do risco quando materializado, podendo ser medido quantitativa e/ou qualitativamente.

“Indicador de Risco” (KRI – Key Risk Indicator): instrumento de medição utilizado para monitorar e analisar variações nos riscos estratégicos, possibilitando estimar a manifestação destes. A fonte dos dados do indicador pode ser de origem interna ou externa.

“Matriz de Risco”: representação gráfica dos riscos do negócio identificados pela Companhia. O risco é disposto a partir do resultado da avaliação da sua criticidade, considerando o eixo de impacto versus a probabilidade de materialização.

“Plano de Ação”: tratamento aplicado aos fatores de risco com o objetivo de minimizar o impacto e/ou a probabilidade da sua materialização ou ainda, não permitir o aumento da sua criticidade.

“Plano de Trabalho de Gestão de Riscos”: documento elaborado pela área de Gestão de Riscos contendo o planejamento periódico (por exemplo, anual) das atividades a serem executadas, reportadas e apresentadas, prazos, recursos necessários e atribuições dos responsáveis.

“Resposta ao Risco”: definição do tratamento que a Companhia dará ao fator de risco. Como resposta, pode-se optar por aceitar, eliminar, reduzir ou transferir.

“Apetite a Risco”: grau de exposição a Riscos que a Companhia está disposta a aceitar para atingir seus objetivos.

“Tolerância a Risco”: percentual do apetite a risco estabelecido pela organização que, quando atingido, aciona a Governança para a reavaliação dos riscos.

“Area de Gestão de Riscos”: área da Companhia que responde diretamente à presidência, responsável pela gestão dos riscos conforme atribuição desta política.

3. DIRETRIZES

O processo de gerenciamento de riscos deve estar integrado à cultura, valores, estratégia, tomada de decisão, operação e estrutura organizacional, promovendo a identificação oportuna

e o adequado tratamento dos riscos.

É papel do Conselho de Administração, Comitê de Auditoria e Riscos, demais órgãos estatutários ou de assessoramento do Conselho de Administração, Presidência, e Diretoria disseminar a cultura de gerenciamento de riscos a todos os colaboradores da Marisa, bem como supervisionar o processo.

O processo de tomada de decisão deve considerar e avaliar os riscos existentes com o propósito de aproveitar as oportunidades, proteger contra as ameaças, criar e gerar valor à Marisa.

O processo de gerenciamento de riscos deve ser avaliado anualmente, promovendo a melhoria contínua e assegurando a eficácia da gestão dos riscos do negócio.

Os riscos corporativos, após identificados e avaliados, considerando os esforços de mitigação existentes, devem ter seu tratamento e monitoramento definidos (Resposta ao Risco).

Os critérios de elegibilidade dos Donos dos Riscos são estabelecidos de acordo com o entendimento do contexto do risco e do cenário da Companhia, no entanto é recomendado que sejam cargos executivos.

3.1 PROCESSO

O processo de gerenciamento de riscos compreende a identificação e a análise dos riscos que comprometam o negócio e o atendimento dos objetivos estratégicos da Companhia, formando uma base de riscos que devem ser tratados e gerenciados.

Os riscos e fatores de riscos são avaliados por seu impacto nos objetivos e resultados da Companhia, e sua probabilidade de ocorrência, utilizando metodologias de mensuração quantitativa e/ou qualitativa.

A escala de impacto é avaliada em sete pilares, quais sejam: financeiro, continuidade e perenidade, operação, conformidade, imagem e reputação, meio ambiente e comunidade, saúde e segurança, contendo cinco níveis de ponderação: mínimo, baixo, moderado, significativo e alto. O Procedimento de Gerenciamento de Riscos define os eventos resultando em cada ponderação de impacto por pilar analisado.

A escala de probabilidade por materialização do risco define cinco níveis de ponderação, descritos abaixo:

Análise de Probabilidade e Frequência estimada de materialização do risco			
Escala	Probabilidade	Frequência	Descrição
5 Quase Certo	90% < 100%	Mais de 1 vez por mês	É quase certo que irá acontecer. Histórico amplamente conhecido e com eventos recentes.
4 Provável	70% < 90%	Mais de 1 vez por semestre até 1 vez por mês	É mais provável que o evento ocorra do que não ocorra. Histórico parcialmente conhecido.
3 Possível	30% < 70%	1 vez por ano a uma vez por semestre	Pode ocorrer em algum momento, frequência reduzida. Existe histórico de ocorrência.
2 Baixa	10% < 30%	Menos de uma vez por ano	Chance pequena de que o evento ocorra
1 Raro	< 10%	Menos de uma vez em 5 anos	Chances remotas (raras) de que o evento ocorra

O resultado da avaliação é apresentado por meio de uma abordagem de matriz bidimensional que estabelece os níveis de criticidade dos riscos, a partir da combinação dos eixos de impacto e probabilidade, sendo cada um deles subdividido a partir de sua escala de 5 níveis da Régua de Impacto versus Probabilidade.

Os níveis de criticidade identificados referem-se ao potencial dano à Companhia, conforme exposto abaixo:

Nível de Criticidade	Descrição
Alto	Alto grau de certeza de impacto negativo nos lucros e/ou à imagem da Companhia e/ou nos objetivos estratégicos.
Significativo	Potencial de impacto negativo nos lucros e/ou à imagem da Companhia e/ou nos objetivos estratégicos.
Moderado	Impacto negativo moderado nos lucros e/ou à imagem da Companhia e/ou nos objetivos estratégicos.

Baixo	Impacto negativo baixo nos lucros e/ou à imagem da Companhia e/ou nos objetivos estratégicos.
--------------	---

A seguir é demonstrado um exemplo de representação gráfica em matriz bidimensional, ilustrando a divisão de cada nível de criticidade:

Impacto	Alto					
	Significativo					
	Moderado					
	Baixo					
	Mínimo					
		Raro	Baixo	Possível	Provável	Quase Certo
		Probabilidade				

Após o processo de avaliação dos riscos inerentes, devem ser definidos quais serão priorizados, para posterior definição do tratamento (alinhado à resposta ao risco) e como estes devem ser monitorados e comunicados às diversas partes envolvidas.

O tratamento dos riscos inerentes consiste em definir qual resposta será aplicada, entre aceitá-lo, eliminá-lo, reduzi-lo ou transferi-lo. A decisão deve ser tomada individualmente por risco, levando em consideração o grau de apetite a risco da Companhia. O Procedimento de Gerenciamento de Riscos detalhará os processos de classificação por tratamento de risco.

Caso a resposta definida para um risco seja aceitá-lo, a decisão deve ser formalmente submetida para aprovação, conforme alçada descrita a seguir:

Criticidade do Risco	Alçada de Aprovação
Alto	Conselho de Administração
Significativo	Presidente
Moderado	Diretoria / Head
Baixo / Mínimo	Gerência

O Comitê de Auditoria e Riscos deve ser informado sobre a aceitação de todos os riscos Altos e Significativos, com detalhes do racional de classificação e dos motivos pelo não tratamento dos riscos. . Todos os riscos aceitos devem ser reavaliados formalmente pela Companhia em um período máximo de 12 (doze) meses, a fim de se verificar se as condições que impediram o seu devido tratamento ainda persistem, ou se haveria novas alternativas de abordagem.

Area de Gestão de Riscos deve realizar reportes periódicos de riscos ao Comitê de Auditoria e Riscos, e este, por sua vez, a seu critério, reportar ao Conselho de Administração, com os seguintes objetivos, dentre outros:

- emitir alertas quando ações corretivas ou de contingência se fizerem necessárias;
- apontar riscos que precisam de atenção;
- compartilhar boas práticas;
- alertar as áreas de Auditoria Interna e Compliance sobre riscos e/ou processos, que podem precisar de revisão nos controles internos; e
- monitorar a disciplina de execução dos planos de ação, prazos e seus respectivos responsáveis.

O processo de monitoramento deve ser realizado pela área de Gestão de Riscos utilizando informações provenientes do trabalho das áreas de Compliance, Segurança da Informação e Auditoria Interna. Também deve contar com o apoio das áreas de negócio, uma vez que novos riscos identificados devem ser informados e encaminhados à área de Gestão de Riscos para posterior inserção dos dados na matriz de riscos.

O processo descrito deve ser documentado em uma matriz de riscos, que deve ser revisada anualmente ou a qualquer momento oportuno, considerando fatos relevantes, alterações na estratégia e/ou mudança no nível de impacto e probabilidade dos riscos existentes.

4. RESPONSABILIDADES

CONSELHO DE ADMINISTRAÇÃO

- Definir o apetite a riscos, ou seja, o grau de exposição a Riscos que a Companhia está disposta a aceitar para atingir seus objetivos;
- Definir a estratégia da Companhia para atendimento de seus objetivos de negócio;
- Conhecer o portfólio de riscos estratégicos;
- Aprovar os riscos priorizados e as devidas estratégias de tratamento e/ou monitoramento;
- Aprovar a resposta ao risco caso esta seja aceitar e o risco tenha criticidade “Alto”;
- Aprovar a Política de Gestão de Riscos, assim como suas revisões;
- Supervisionar, com suporte dos comitês estatutários, a efetividade da estrutura e do processo de Gestão de Riscos da Marisa; e,
- Aprovar as atribuições dos departamentos de auditoria interna, controles internos, riscos e compliance.
- Garantir que os mecanismos de avaliação de desempenho e a estrutura remuneratória adotados pela Companhia não incentivem comportamentos capazes de comprometer a efetividade do Sistema de Controles Internos e da Estrutura de Gestão de Riscos.

COMITÊ DE AUDITORIA e RISCOS - ESTATUTÁRIO

- Revisar a Política de Gestão de Riscos Corporativos, formulando e avaliando propostas de alterações e aperfeiçoamento, e recomendando a sua aprovação ao Conselho de Administração;
- Reportar os planos de trabalho e as ações da Auditoria Interna diretamente ao Conselho de Administração;
- Acompanhar de forma sistemática a gestão de riscos e o cumprimento de seus objetivos;

- Avaliar as atividades da área de Gestão de Riscos e Controle Interno da Companhia;
- Avaliar a efetividade e a suficiência dos sistemas de controles e de gerenciamento de riscos operacionais;
- Acompanhar as mudanças na avaliação da criticidade dos riscos e reportar as variações significativas ao Conselho de Administração;
- Monitorar a execução dos planos de ação para o tratamento dos riscos, prazos e seus respectivos responsáveis;
- Recomendar à Diretoria a correção ou aprimoramento de políticas, práticas e procedimentos identificados no âmbito de suas atribuições;
- Avaliar, sob o enfoque de riscos, o plano de negócio da Companhia, e a aderência correspondente ao apetite por risco; e,
- Recomendar ações que facilitem os processos de tomada de decisões estratégicas relacionadas à gestão de riscos.

DIRETORIA

- Identificar riscos preventivamente e fazer sua necessária gestão, avaliando a probabilidade de ocorrência e adotando medidas para sua prevenção e minimização;
- Aprovar a resposta ao risco, caso esta seja aceitar, e o risco tenha criticidade “Moderado”
- Validar os riscos inerentes à operação da Marisa levando em consideração o seu impacto e sua probabilidade de ocorrência;
- Contribuir para a elaboração do relatório de riscos corporativos;
- Comunicar todos os riscos conhecidos à área de GESTÃO DE RISCOS, sejam eles novos ou não; e,
- Acompanhar e interferir, caso necessário, o processo de execução dos Planos de Ação definidos.

PRESIDENTE

- Implementar as estratégias e diretrizes da Companhia aprovadas pelo Conselho de Administração;
- Respeitar as diretrizes de governança corporativa e políticas, assim como monitorar sua observância;

- Identificar riscos preventivamente e fazer sua necessária gestão, avaliando a probabilidade de ocorrência e adotando medidas para sua prevenção e minimização;
- Aprovar a resposta ao risco, caso esta seja aceitar, e o risco tenha criticidade “Significativo”;
- Propor e implementar sistema de controles internos incluindo políticas e limites de alçada, alinhado ao nível de apetite e tolerância ao risco;
- Propor indicadores de sustentabilidade de suas operações, considerando fatores ambientais e sociais na execução de suas atividades; e,
- Patrocinar a implantação da gestão de riscos corporativos na Companhia.

DONOS DOS RISCOS

- Contribuir para elaboração do relatório de riscos corporativos;
- Comunicar todos os riscos conhecidos à área de Gestão de Riscos sejam eles novos ou não;
- Estabelecer os Planos de Ação e assegurar a implementação deles;
- Elaborar as fichas de riscos e atualizá-las sempre que necessário;
- Revisar, periodicamente, o detalhamento técnico do risco, dos seus fatores, a avaliação do risco (impacto e probabilidade) e a resposta, considerando alterações nas ações mitigatórias existentes, conclusão da implantação dos planos de ação e de contingência, e resultados das avaliações dos processos (ambiente de controle) relacionados ao risco;
- Efetuar reportes periódicos à área de Gestão de Riscos sobre o acompanhamento do risco sob sua responsabilidade (mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica, bem como se identificados riscos não mapeados); e,
- Quando solicitado, efetuar reporte à Presidência, ao Comitê de Auditoria e Riscos e ao Conselho de Administração.

GESTÃO DE RISCOS

- Estabelecer e atualizar processos e políticas a serem utilizados na gestão de Risco

Corporativo;

- Elaborar e revisar, periodicamente, a Governança de Gestão de Riscos;
 - Propor critérios para identificação, avaliação e classificação dos riscos;
 - Propor e revisar a metodologia para o cálculo do apetite a risco;
 - Atuar em conjunto com a Presidência, Diretorias, ao Comitê de Auditoria e Riscos, e Conselho de Administração na discussão sobre a definição do apetite a risco e os níveis de tolerância aceitáveis;
 - Elaborar, revisar e atualizar o portfólio de riscos sempre que houver atualizações na estratégia e ou no modelo de negócio, bem como mudanças significativas nos processos, e ou nos sistemas, ou no mínimo bianualmente;
 - Auxiliar na definição dos Donos dos Riscos;
 - Assessorar o Dono do Risco na definição de plano(s) de ação e/ou de contingência e na criação de indicadores para o monitoramento dos níveis de exposição dos riscos;
 - Acompanhar mudanças relevantes na criticidade dos riscos e reportá-las à Presidência, às Diretorias, ao Comitê de Auditoria e Riscos e ao Conselho de Administração;
 - Consolidar a avaliação de Riscos;
-
- Elaborar relatórios e reportes acerca dos resultados do processo de Gestão de Riscos à Presidência, às Diretorias, ao Comitê de Auditoria e Riscos e ao Conselho de Administração;
 - Apoiar os gestores Responsáveis na definição e execução dos planos de ação e prazo necessários para tratamento dos Riscos e notificar os descumprimentos de acordo com as devidas alçadas; e
 - Disseminar a cultura de Gestão de Riscos, conscientizando sobre a importância da gestão de riscos e a responsabilidade inerente aos colaboradores.

AUDITORIA INTERNA (Atribuições específicas do processo de Gestão de Riscos)

- Reportar-se diretamente ao Conselho de Administração, o qual é responsável pela aprovação de suas atribuições, por meio do Comitê de Auditoria e Riscos e,

administrativamente, ao Presidente da Companhia;

- Apoiar a Gestão de Riscos por meio de trabalhos especiais de auditoria interna na avaliação dos controles e dos processos atrelados aos riscos estratégicos e de negócio;
- Prover o Conselho de Administração, o Comitê de Auditoria e Riscos e o Presidente com avaliações independentes, imparciais e tempestivas sobre a efetividade do gerenciamento dos riscos e dos processos de governança, da adequação dos controles e do cumprimento das normas e regulamentos associados às operações da Companhia, sendo que a Auditoria Interna possui caráter independente tendo suas atribuições aprovadas pelo Conselho de Administração;
- Subsidiar a área de Gestão de Riscos sobre os principais riscos e controles vigentes identificados durante suas revisões anuais por diversos processos de negócio, dentro de seu papel de avaliador independente do ambiente de controles internos e do desempenho das áreas de negócio;
- Efetuar testes nos controles internos com objetivo de avaliar a sua efetividade;
- Conhecer os riscos estratégicos, bem como quais deles foram priorizados e considerá-los como um dos critérios para a elaboração/atualização do Plano de Auditoria Interna.

5. DISPOSIÇÃO FINAL

O disposto acima se aplica para toda a Companhia a partir da publicação desta Política.

6. INFORMAÇÃO DOCUMENTADA

Processo
Estatuto Social da Companhia
Código Marisa de Conduta Ética
ISO 31000:2018
Código Brasileiro de Governança Corporativa
Instrução CVM 552

Instrução CVM 586
Regulamento do Novo Mercado (B3)
Resolução 4557 BACEN
Formulário de Referência.
Política de Segurança da Informação
Procedimento - Processo de Gestão de Risco à Segurança da Informação

7. REVISÃO E ATUALIZAÇÃO

Esta política tem vigência a partir da sua aprovação pelo Conselho de Administração da Companhia e sua divulgação, e deverá ser revista e atualizada em intervalos não superiores a 2 (dois) anos ou sempre que as atividades previstas modificarem.

8. HISTÓRICO DO DOCUMENTO

Versão	Data atualização	Autor	Resumo das modificações
03	02/12/2024	Millena Pacheco	Criação do documento.
03	11/12/2024	Fernanda Hoelz	Revisão do documento.

9. CIENCIA ALTA ADMINISTRAÇÃO E APROVADORES

Aprovadores	Assinaturas
Edson Salles Abuchaim Garcia Diretor-Presidente	

Millena Andreza Zambom Pacheco Gerente de Gestão de Riscos e Controles Internos	
---	--