Política de Gestão de Riscos

Departamento	Data de atualização	Código
Compliance	13/03/2023	PLCOMP11

Sumário

1. Resumo

Para referência e facilitar a compreensão de seus termos, a seguir apresentamos o resumo das principais orientações contidas nesta Política de Gestão de Riscos ("Política"). Ressaltamos, porém, que a leitura integral da Política é necessária:

O que fazer

- Ter conhecimento acerca das disposições desta Política e disseminar a cultura de gestão de riscos da Companhia, contribuindo para uma gestão eficiente de riscos em seu âmbito;
- Observar as diretrizes e respectivas responsabilidades previstas nesta Política, reconhecendo que a estrutura de gestão de riscos da Companhia é descentralizada, de modo a aproveitar e potencializar a gestão do conhecimento técnico e perfil dos profissionais de cada área [itens 4, 5 e 6];
- Identificar e tratar de maneira adequada riscos que possam afetar os objetivos da Companhia, seguindo a classificação, avaliação e priorização realizadas pela Companhia, e observando o tratamento a ser dado ao risco, conforme o caso (diminuir, evitar, compartilhar ou reter) [Item 6.4];
- Contribuir para o acesso tempestivo a informações quanto aos riscos aos quais a Companhia está exposta, contribuindo para a tomada de decisão pelos responsáveis, em todos os níveis, aumentando a probabilidade do alcance dos seus objetivos e redução a níveis aceitáveis, conforme o caso;
- Registrar e documentar as etapas do processo de gestão de riscos;

O que não fazer

- Tomar decisões, em qualquer nível hierárquico, que desrespeitem o processo de gestão de riscos disciplinado por esta Política, especialmente com relação ao tratamento a ser dado aos riscos (diminuir, evitar, compartilhar ou reter);
- Não seguir planos de ação definidos no âmbito da gestão de riscos;
- Deixar de registrar e documentar as etapas do processo de gestão de riscos;

2. Objetivo

Estabelecer as diretrizes e procedimentos para identificação, avaliação, monitoramento, gerenciamento e tratamento dos riscos de forma compatível à natureza, porte, complexidade, estrutura, perfil e tolerância de risco ao modelo de negócios da Companhia, minimizando seus impactos.

3. Abrangência

Aplicável a todos os administradores, incluindo o Conselho de Administração e Comitê de Auditoria, Finanças e Riscos Estatutário ("CARF"), Diretores e colaboradores, independentemente de nível hierárquico e/ou posição de liderança, que, direta ou indiretamente, participam do processo de gestão de riscos da Companhia.

4. Escopo

A Gestão de Riscos deve responder a gestão de incertezas, ameaça de eventos ou ações que possam impactar adversamente os negócios da Companhia.

Dessa maneira os principais de riscos para os quais se busca proteção são:

- Riscos de Conjuntura e Mercado
- Riscos Financeiros
- Riscos Regulatórios
- Riscos de Conformidade (*Compliance*)
- Riscos Legais
- Riscos Socioambientais
- Riscos de Tecnologia e Segurança da Informação
- Riscos da Operação
- Riscos de Reputação e Imagem

O processo de gestão de riscos visa assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo tanto às informações quanto aos riscos aos quais se está exposto, de forma a aumentar a probabilidade do alcance dos seus objetivos e reduzi-los aos níveis aceitáveis.

A estrutura de gestão de riscos da Companhia é descentralizada, para aproveitar e potencializar a gestão do conhecimento técnico e perfil dos profissionais de cada área. Os responsáveis pelos processos devem identificar e tratar os riscos que possam afetar os objetivos da Companhia.

5. Responsabilidades

A disseminação da cultura de gestão de riscos da Companhia é responsabilidade de todos os colaboradores, que têm o papel de contribuir para uma gestão eficiente.

Sendo assim, e sem prejuízo das atribuições legais, regulatórias e aquelas previstas no Estatuto Social e nas normas internas da Companhia, em especial nos respectivos regimentos internos, quando aplicável,

a estrutura de gestão de riscos da empresa considera a atuação conjunta dos órgãos de governança corporativa e de gestão que possuem as responsabilidades a seguir:

5.1. Conselho de Administração

a. Aprovar as diretrizes da presente Política, bem como sua efetiva implementação;
b. Acompanhar o cumprimento dos parâmetros implementados para gestão dos riscos, com o apoio dos Comitês de assessoramento, do departamento de *Compliance* e o responsável pela auditoria interna;
c. Estabelecer o nível de apetite a riscos e acompanhar, com assessoria dos Comitês, as exposições resultantes das decisões tomadas na condução dos negócios da Companhia;
d. Conscientizar e incentivar os gestores na busca de saídas econômicas para redução da probabilidade de eventos de risco ou para mitigar suas consequências;
e. Patrocinar a cultura de gestão de riscos com apoio da Diretoria Executiva e do CARF, o qual assumirá a liderança no acompanhamento do cumprimento dessa Política;
f. Garantir que o CARF tenha orçamento próprio para a contratação de consultores para assuntos contábeis, jurídicos ou outros temas, quando necessária a opinião de um especialista externo; e, Avaliar anualmente, diretamente ou por meio do CARF, a estrutura e o orçamento da Auditoria Interna, que deverá ser suficiente ao desempenho de suas funções.

5.2. Comitê de Auditoria, Finanças e Riscos Estatutário (CARF)

a. Acompanhar o cumprimento dos parâmetros implementados para gestão dos riscos, com o apoio da área de *Compliance* e Gestão de Riscos;
b. Avaliar e aprovar o Plano Anual de Gestão de Riscos e de Auditoria Interna, bem como avaliar anualmente a estrutura e o orçamento da Auditoria Interna, que deverá ser suficiente ao desempenho de suas funções; e
c. Suportar às decisões do Conselho de Administração no que tange a mitigação dos riscos.

5.3. Diretoria Executiva

a. Atuar diretamente na gestão dos riscos inerentes às suas atividades (identificar, avaliar e tratar);
b. Informar à área de *Compliance* sobre a identificação de novos riscos ou eventos que sejam relevantes e suas respectivas evoluções;
c. Reportar semestralmente ao CARF o nível de exposição dos principais riscos identificados;
d. Suporte às decisões do Conselho de Administração no que tange a mitigação dos riscos;
e. Apoiar o subsídio de recursos (humanos, financeiros e tecnológicos) para a implementação de controles internos efetivos e estratégias de mitigação de riscos; e,

f. Acompanhar a implementação dessa Política, sugerir melhorias e assegurar a existência de plano de administração de crises que permita a Companhia ultrapassá-las de forma segura.

5.4. *Compliance* e Gestão de Riscos

a. Sugerir o Programa de Gestão de Riscos e o Plano Anual de Auditoria Interna;
b. Aplicar metodologia de Gerenciamento de Riscos;
c. Monitorar o cumprimento do apetite ao risco no gerenciamento de riscos; dar suporte às áreas na identificação e tratamento de riscos, principalmente, através do Risk Squad (grupo de trabalho designado pela Diretoria para serem disseminadores da cultura de Gestão de Riscos nas áreas);
d. Coordenar a atualização do mapa de risco e do plano de ação sempre que necessário;
e. Recomendar mecanismos de controle e planos de ação para mitigação dos riscos identificados e elaboração de planos de continuidade de negócios;
f. Reportar, sempre que solicitado pelo CARF, o status do Programa de Gestão de Riscos;
g. Disseminar a cultura da gestão de riscos, controles internos e continuidade de negócio.

5.5. Auditoria Interna

As atividades de Auditoria Interna serão conduzidas por equipe interna independente ou, alternativamente, por empresa especializada, observado que, nesse caso, a empresa deverá ser auditor independente registrada na CVM.

A Auditoria Interna deve ter estrutura e orçamento considerados suficientes ao desempenho de suas funções, conforme avaliação anual realizada pelo Conselho ou pelo CARF.

A Auditoria Interna será responsável por aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controles e governança da Companhia, conforme plano anual sugerido pela área de Compliance, avaliado pelo CARF e aprovado pelo Conselho.

Sem prejuízo do acima exposto e de outras atribuições que venham a ser avaliadas pelo CARF e aprovadas pelo Conselho, compete à Auditoria Interna:

a. Reportar periodicamente à Alta Administração os resultados das avaliações dos riscos estratégicos e processos de gerenciamento de riscos;
b. Recomendar mecanismos de controle e planos de ação para mitigação dos riscos identificados e elaboração de planos de continuidade de negócios;
c. Monitorar o cumprimento do apetite ao risco no gerenciamento de riscos; e,
d. Disseminar a cultura da gestão de riscos, controles internos e continuidade de negócio.

5.6. Gestores das áreas correlacionadas aos riscos estratégicos e dos processos

a. Implementar controles internos recomendados pela área de riscos;
b. Assegurar a implementação dos planos de ação que visam mitigar os riscos;
c. Aplicar as metodologias de gerenciamento de risco;
d. Identificar, documentar e comunicar às áreas responsáveis todas as perdas operacionais resultantes de falha, deficiência ou inadequação de processos e controles internos, pessoas e sistemas ou eventos externos; e,
e. Cumprir as diretrizes definidas para o gerenciamento de risco e o apetite a risco.

6. Diretrizes

As diretrizes aqui apresentadas definem e caracterizam as macro etapas do processo de Gestão de Riscos que correspondem:

6.1. Definição do Apetite de Risco e Tolerância

O Conselho de Administração define o Grau de exposição a riscos que a Companhia está disposta a tolerar na implementação de suas estratégias de negócio e realização de suas atividades, a fim de atingir seus objetivos estratégicos exercendo seu Propósito, com visão de futuro e alinhado aos valores e cultura da Companhia, considerando os seguintes critérios:

- Os níveis de prejuízos esperados e não esperados que possam ser aceitos;
- Padrões setoriais, padrões de desempenho de melhores práticas etc.;
- Preferências e expectativas das partes interessadas;
- Desempenho esperado dos negócios (retorno sobre o capital);
- Volatilidade dos lucros que estamos preparados a aceitar;
- A quantidade de capital que estamos preparados para colocar em risco;
- A cultura da organização;
- Experiência da administração juntamente com as habilidades de gerenciamento e controle de risco; e,
- Prioridades estratégicas de prazos mais longos.

Riscos Inaceitáveis: A Companhia fará seus melhores esforços para evitar exposição a riscos inaceitáveis, tais como atividades que possam resultar em danos a reputação, atividades ilegais, violação de pontos

regulatórios, não cumprimento de mandatos e violações de conduta graves. Uma vez que o risco seja identificado, ele será elencado pela Diretoria para o departamento de *Compliance* e CARF com a urgência apropriada.

6.2. Identificação e Análise dos Riscos

Com base no resultado do Apetite de Riscos, os riscos corporativos relacionados à Companhia são identificados e analisados para assegurar que quaisquer materializações que venham a ocorrer sejam conhecidas previamente e geridas em um nível aceitável.

Para identificar e descrever os riscos, a Companhia deve utilizar entrevistas com gerentes, executivos e conselheiros, coleta de dados, análise de evidências, documentos, pesquisas e validações junto as áreas técnicas envolvidas. Como resultado haverá uma lista de riscos associada ao escopo e ao cenário definido.

Para fins de categorização, os Riscos Corporativos devem ser divididos entre Estratégicos, Operacionais e Externos e devem ser classificados conforme o escopo definido nesta Política.

Essa avaliação resulta no mapa de riscos da Companhia, proporcionando um mecanismo para as etapas de avaliação e priorização dos mesmos e, consequentemente, uma ferramenta de direcionamento dos esforços para minimizar os riscos.

6.3. Avaliação e Priorização

Concluída a análise e obtida a classificação do risco, bem como verificado se o mesmo está ou não aderente ao Apetite estabelecido, ele é enquadrado em uma matriz de priorização.

As avaliações dos riscos corporativos compreendem a identificação e a análise dos riscos sobre os aspectos financeiros, de recursos, reputacionais e de integridade, formando uma base para determinar como os riscos devem ser gerenciados. A Diretoria e a área de *Compliance* devem avaliar os eventos de risco por seu impacto e sua probabilidade de ocorrência.

O critério de impacto considera as diretrizes da administração em relação ao possível impacto financeiro (perda) relacionado à imagem e à reputação da Companhia. O critério da probabilidade considera a magnitude em que a Companhia está exposta ou desprotegida em relação a diversos fatores externos e internos.

A avaliação final do grau de exposição da Companhia a cada Risco será definida em função da combinação entre o impacto e a probabilidade, demonstrada na tabela a seguir.

		Impacto				
		Muito baixo	**Baixo**	**Médio**	**Alto**	**Muito alto**
Probabilidade	**Muito baixo**	Muito baixo	Muito baixo	Muito baixo	Baixo	Médio
	Baixo	Muito baixo	Baixo	Baixo	Médio	Alto
	Médio	Muito baixo	Baixo	Médio	Alto	Muito alto
	Alto	Baixo	Médio	Alto	Alto	Muito alto
	Muito alto	Médio	Alto	Muito alto	Muito alto	Muito alto

Riscos Muito Altos indicam que ações de respostas para diminuir a probabilidade e o impacto a níveis aceitáveis são necessárias e urgentes.

Riscos Altos indicam que, na impossibilidade de redução do impacto ou probabilidade, o risco requer ações preventivas ou corretivas imediatas e monitoramento, inclusive por parte do Conselho.

Riscos Médios indicam que pode ser aceito ou tratado de acordo com a avaliação dos responsáveis quanto a necessidade de tratamento dos riscos para reduzi-los a níveis ainda mais baixos.

Riscos Baixos e Muito Baixos indicam que o risco inerente já está dentro da tolerância a risco, salvo risco inaceitáveis.

6.4. Tratamento

Com base nos resultados obtidos na etapa de avaliação e priorização, a Diretoria deve aprovar o tratamento a ser dado ao risco: **Diminuir**, **Evitar**, **Compartilhar** ou **Conviver**.

Caso a opção seja reter o risco, devem ser estabelecidas métricas de monitoramento pela Diretoria.

Para os riscos com criticidade Média ou Baixa, os Planos de Ação devem ser definidos e monitorados pela Diretoria com o acompanhamento da área de Gestão de Riscos *e* com a definição de responsáveis e prazo de conclusão.

Todas as ações devem ter um gestor, que ficará responsável pelo estudo técnico de viabilidade operacional e financeira da ação.

Além dos Planos de Ação, os riscos apontados devem ser examinados pela Diretoria com o acompanhamento do departamento de *Compliance*, a fim de buscar soluções que atuem na reversão do impacto possivelmente já gerado, e classificados como elegíveis a ação corretiva e melhoria no processo, cujo objetivo é evitar ou reduzir a chance de reincidência do evento.

6.5. Comunicação e Monitoramento

A Companhia deve comunicar, de forma clara e objetiva a todas as partes interessadas, os resultados das etapas do processo de Gestão de Riscos, de forma a contribuir para o entendimento da situação atual e da eficácia dos Planos de Ação.

A Diretoria em conjunto com o departamento de *Compliance* deve garantir, por meio de atividades contínuas de monitoramento e a avaliação independente a eficácia do gerenciamento dos riscos corporativos.

Todas as etapas do processo de gestão de riscos devem ser registradas e ter sua documentação suporte e evidências armazenadas pelo departamento de *Compliance.*

6.6. Revisão e Atualização

O processo de gerenciamento de riscos da Companhia é contínuo e assim, a gestão por classe dos riscos e níveis de apetite e tolerância serão constantemente revisitados, devendo o mapa de riscos deve ser atualizado com a periodicidade de 3 (três) anos ou se houver a identificação de novos riscos ou eventos que sejam relevantes.

7. **Prazo**

Esta política tem validade a partir da data de sua publicação, podendo ser alterada a qualquer tempo e critério pela área de *Compliance*, que deverá submeter as alterações para análise do CARF e aprovação do Conselho de Administração.

8. **Histórico de mudanças**

Revisão	Descrição	Data
1.0	- Elaboração da PLCOMP11-Política de Gestão de Riscos	27/11/2020

2.0	- Readequação geral da Política de Gestão de Riscos de acordo com modelo de negócio da Companhia; - Alteração para novo modelo visual	04/11/2021
3.0	- Adequação para matriz 5x5 - Atualização das responsabilidades do CARF - Nova classificação de natureza dos riscos - Ajustes na estrutura e atribuições da Auditoria Interna	13/03/2023

CYRELA

São Paulo, 13 de março de 2023.

Miguel Maia Mickelberg
Dir. Financeiro e Dir. de RI

Rafaella Carvalho
Dir. Jurídica