Manual de Processos, Normas e Políticas

Gestão de Riscos

ÍNDICE

1. OBJETIVO 3
2. APLICABILIDADE 3
3. DEFINIÇÕES 3
4. DIRETRIZES 4
4.1. Abordagem 5
5. GESTÃO DE RISCOS 6
5.1. Entendimento do ambiente e objetivos 6
5.2. Identificação de eventos e riscos 7
5.3 Avaliação de riscos e controles 7
5.4 Resposta ao risco 8
5.5 Informação, Comunicação e monitoramento contínuo 8
6. ATRIBUIÇÃO E RESPONSABILIDADE 9
6.1. Conselho de Administração 9
6.2. Comitê de Auditoria e Riscos 10
6.3. Diretoria 10
6.4. Área de Gestão de Riscos 10
6.5. Área de Auditoria Interna 11
6.6. *Risk Owners* 11
7. VIGÊNCIA 12
8. SANÇÕES 12
9. ATUALIZAÇÕES DESTA POLÍTICA 12
ANEXO I – DICIONÁRIO DE RISCOS 13

1. OBJETIVO

O objetivo desta Política é estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de gestão dos riscos da Moura Dubeux S.A ("Companhia" ou "organização") e suas controladas.

2. APLICABILIDADE

Esta Política é aplicável à Companhia e às suas controladas, devendo ser observada por seus respectivos conselheiros, diretores, membros de comitê, colaboradores, administradores e prestadores de serviços. Devendo ser cumprida e ser fonte de consulta em caso de dúvidas.

3. DEFINIÇÕES

Risco: possibilidade de ocorrência de um evento capaz de impactar os objetivos e resultados da Companhia. Envolve a quantificação e a qualificação da incerteza, tanto no que diz respeito às perdas quanto aos ganhos da organização.

Risco estratégico: risco que, em caso de ocorrência, possa impactar os objetivos estratégicos da organização. Está geralmente associado aos eventos internos ou externos que afetam a capacidade de execução da estratégia de negócio da organização.

Risco do processo: risco que, em caso de ocorrência, possa impactar os objetivos táticos (operacionais) da organização. Está geralmente associado a falhas, deficiências ou inadequações de processos, pessoas ou sistemas.

Risco é inerente: que se origina da natureza própria da conta ou do tipo de operação analisada.

Risco residual: risco que resulta depois de implementados atividades de controle.

Apetite ao risco: é o nível de risco com limites estabelecidos que a organização está disposta a assumir na busca e na realização de seus objetivos.

Análise de impacto/vulnerabilidade de risco: é um dos fatores considerados para definição da matriz de impacto de risco, cuja definição da severidade é mensurada como sendo diretamente proporcional ao potencial de impacto do risco. O impacto é avaliado considerando o desempenho econômico-financeiro, a imagem da organização e os fatores sociais, ambientais, de conformidade e estratégicos da organização.

Análise de probabilidade de risco: é um dos fatores considerados para definição da matriz de impacto de risco, cuja definição da severidade é mensurada como sendo diretamente proporcional à probabilidade de ocorrência do risco.

Matriz de risco: também conhecida como mapa de calor (*heatmap*), é a representação visual do efeito agregado dos níveis de exposição ao risco em dois eixos de análise de impacto e de probabilidade.

Risk Owner: responsável (gestor ou executivo) que tem a autoridade para executar a gestão de riscos em diferentes áreas de negócio dentro da organização. A atribuição da responsabilidade pode ser compartilhada a nível tático (operacional ou gestor direto) e estratégico (executivo).

Controle interno: é uma estrutura implementada para garantir a eficiência operacional e fornecer segurança razoável de que os objetivos organizacionais serão alcançados. É estabelecido por meio de um conjunto de diretrizes, procedimentos, conferências e trâmites de informações operacionalizados de forma integrada.

Atividade de controle: é uma ação aplicada para responder ao risco, reduzindo o impacto ou a probabilidade dos efeitos de sua materialização.

Plano de ação: é o planejamento de uma ação ou o conjunto de ações necessárias para atingir a atividade de controle em resposta ao risco. É criado por meio de métricas desenvolvidas para reduzir o nível de exposição ao risco.

Matriz de solução: é a representação visual do efeito agregado em dois eixos de análise. Considera esforços e benefícios para implementação do plano de ação em resposta aos riscos.

4. DIRETRIZES

O risco é inerente a qualquer negócio. A sua administração adequada é um elemento-chave para a continuidade desse negócio. Por isso, a Companhia está empenhada em manter um modelo de governança aderente às melhores práticas do mercado para assegurar o atingimento dos seus objetivos e o desempenho do seu negócio de forma sustentável, responsável e transparente em benefício das suas partes interessadas. Isso se reflete em políticas, procedimentos, normas, leis e dispositivos regulatórios a que esteja submetida.

Nesse sentido, a gestão de riscos corporativos é vista pela Companhia como a ferramenta para subsidiar os agentes de governança para que os riscos e os seus impactos sejam considerados no processo de tomada de decisão.

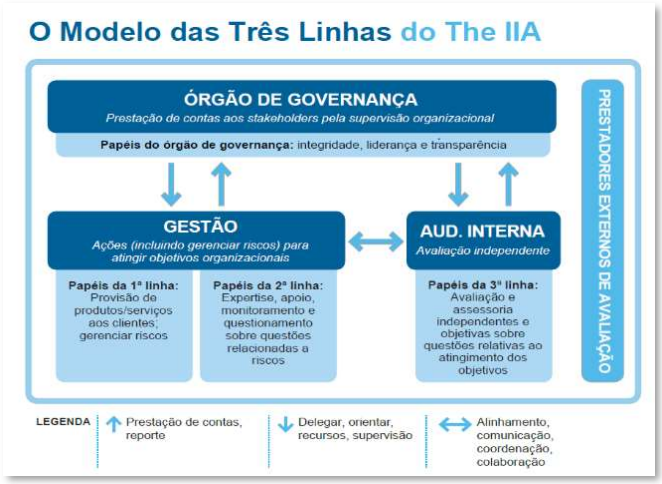
Um sistema estruturado de gestão de riscos possibilita que a organização identifique oportunidades de ganhos e redução da probabilidade de perdas, permitindo que a tomada de decisão esteja alinhada à estratégia e ao apetite ao risco estabelecido pela Alta Administração.

Para a consecução dos objetivos da Companhia, é necessária a participação ativa dos seus colaboradores na gestão de riscos corporativos, independentemente do nível hierárquico. A compreensão dos seus colaboradores dos riscos envolvidos na execução de suas atribuições no negócio permite manter o sistema de gestão de riscos vivo e em funcionamento para um aprimoramento constante.

Desta forma, o processo de gerenciamento de riscos da Companhia é contínuo e deverá ser revisitado no máximo a cada 2 anos ou se houver a identificação de novos riscos ou eventos relevantes.

4.1. Abordagem

A abordagem metodológica adotada pela Companhia baseia-se no quadro integrado sugerido pelo COSO ERM. Também se baseia em recomendações do Gerenciamento de Riscos Corporativos do IBGC – Instituto Brasileiro de Governança Corporativa, que faz correlação com as 3 linhas de defesa no gerenciamento de riscos corporativos criado pelo *Institute of Internal Auditors* – IIA (organização internacional de referência em temas de auditoria). Esse modelo das três linhas de defesa é assim estruturado:



Fonte: IIA – Institute of Internal Auditors

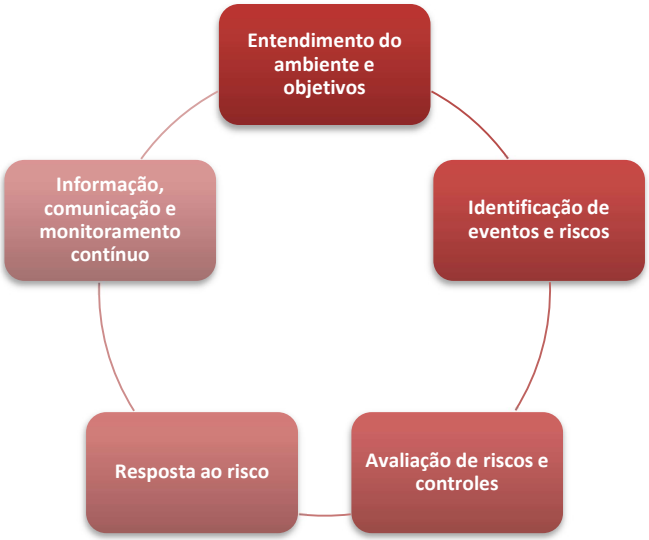
a) A primeira linha deve ser formada por gestores responsáveis pelo funcionamento da organização;

b) A segunda é composta por áreas responsáveis pela conformidade com leis, regulamentos e comportamentos éticos aceitáveis. São elas: controle interno, segurança da informação e tecnologia, sustentabilidade, avaliação da qualidade, gerenciamento de riscos e compliance;

c) A terceira linha é formada pela área de Auditoria Interna, responsável pela asseguração independente (auditoria) de que todas as demais linhas de defesa da organização estão funcionando.

5. GESTÃO DE RISCOS

A execução da gestão de riscos corporativos é estruturada em 5 principais etapas. As etapas sintetizam as fases que devem ser percorridas para a avaliação de riscos de cada processo da organização.



5.1. Entendimento do ambiente e objetivos

O entendimento do ambiente é a etapa em que são coletadas as informações necessárias para verificar se as ações (processos e procedimentos) executadas estão alinhadas aos objetivos da organização. A definição de objetivos é estabelecida pelo Conselho de Administração que, por sua vez, reflete a posição dos acionistas.

Os objetivos são traduzidos em um conjunto de planos e metas com aspectos econômico-financeiros e estratégicos, a serem revistos sempre que houver eventos internos e externos que impactem os resultados projetados. Na definição dos objetivos, é considerado o perfil de risco, ou seja, o equilíbrio do nível de exposição que se aceita incorrer, considerando apetite e tolerância ao risco.

Desse modo, ao estabelecer os objetivos de negócios, eles devem ser amplamente comunicados às partes interessadas para que as potenciais ameaças a esses objetivos sejam identificadas e analisadas.

5.2. Identificação de eventos e riscos

A etapa da identificação de eventos e riscos tem por finalidade identificar e registrar o conjunto de eventos, externos ou internos, que podem comprometer o atingimento dos objetivos. Além disso, são mapeados possíveis causas, efeitos e consequências de cada evento (fatores de risco).

Ainda na etapa de identificação, os riscos são classificados em uma matriz que considera a sua origem, natureza e categoria.

I) Origem: os riscos são classificados como de origem interna ou externa. Os eventos internos estão associados às situações em que a organização consegue intervir diretamente. Nos eventos externos não há uma intervenção direta e, portanto, a organização terá uma ação predominantemente reativa;

II) Natureza: são classificados como de natureza estratégica, financeira, operacional ou conformidade. A classificação por natureza permite organizar os riscos em função da área da organização que será afetada pelos eventos;

III) Categoria: são classificados como de governança, modelo de negócio, político-econômico, crédito, mercado, liquidez, processo, pessoas, informação e tecnologia, conformidade e meio ambiente. A classificação por categoria permite estabelecer uma linguagem comum de riscos dentro da organização.

O dicionário de riscos presente no **Anexo I** apresenta a categorização dos riscos.

5.3 Avaliação de riscos e controles

Essa etapa avalia os riscos identificados considerando causas e consequências. As causas se relacionam à probabilidade de o risco ocorrer e as consequências, ao impacto, caso o evento de risco se materialize. A quantificação do impacto considera o grau de exposição e a natureza (financeiro, operacional e estratégia). Enquanto os eventos são avaliados sob a perspectiva de probabilidade e impacto.

Para avaliação dos riscos, são mensurados efeitos quantitativos e qualitativos, ou a combinação de ambos, e se o risco é inerente (risco que se origina da natureza própria da conta ou do tipo de operação analisada) ou residual (risco que resulta depois de implementados atividades de controle). Além disso, há progressão do risco quando os seus efeitos podem impactar várias áreas.

A correlação entre o potencial impacto e a probabilidade de ocorrência do risco é utilizada para alocar o risco na matriz de impacto. Para isso, são atribuídas notas para cada variável, ponderando no que se denomina mapa de calor. Nele, quanto maior a nota, maior a classificação do risco, que pode variar entre muito alta, alta, média ou baixa.

A Companhia direciona os seus esforços de acordo com essa classificação dos riscos avaliados. Dessa forma, assegura-se que os temas mais relevantes são periodicamente monitorados pelos agentes de governança adequados, com tratativas tempestivas e com a gestão das exposições dentro de níveis aceitáveis.

5.4 Resposta ao risco

A resposta é a etapa para determinar o tratamento a ser dado aos riscos identificados e avaliados. Busca minimizar a sua probabilidade e seu impacto. Essa resposta existe tanto para os riscos que possam afetar adversamente a organização quanto para os riscos que possam trazer benefícios. As respostas possíveis são: quando negativos (ameaças): evitar, mitigar, transferir ou aceitar; quando positivos (oportunidades): explorar, melhorar, compartilhar ou aceitar.

A escolha da resposta considera as possíveis alternativas, o tempo de implementação e o benefício potencial esperado. Assim, elas devem ser a melhor alternativa, considerando o apetite ao risco da Companhia, e a que melhor equilibrará a redução da exposição com os custos relacionados.

A depender da resposta, é criado um plano de ação com a descrição das iniciativas, prazos, esforços e investimentos necessários para a mitigação do risco.

A construção do plano de ação é executada pela primeira linha, com o apoio e monitoramento da segunda linha.

5.5 Informação, Comunicação e monitoramento contínuo

O processo de gestão de riscos deve ser reportado periodicamente aos agentes de governança de forma tempestiva e completa, para acompanhamento e adequada tomada de decisão. A comunicação efetiva assegura que a informação chegará ao conhecimento dos envolvidos de forma a permitir a efetividade no tratamento dos riscos.

Os relatórios auxiliam a área de Auditoria Interna a respeito das áreas de risco da Companhia, informando quais áreas podem precisar de uma revisão nos controles internos, além de sinalizar ao Conselho sobre a vulnerabilidades, deficiências e necessidade de ações corretivas dentro da organização.

As instâncias de monitoramento são realizadas de acordo com pelo nível de criticidade do risco. O monitoramento ocorrerá anualmente, com base no reporte anual dos resultados consolidados em que se compartilha a avaliação do perfil de riscos e a eficácia dos procedimentos regulares de monitoramento.

Nível de Exposição ao Risco		Instância de reporte para monitoramento dos riscos
MA	Muito Alta	Conselho de Administração Comitê de Auditoria e Risco Diretoria Executiva
A	Alta	
M	Média	
B	Baixa	Diretoria Executiva Gerências

Para que toda a Companhia esteja empenhada em manter um modelo de governança aderente às melhores práticas de mercado, são realizados treinamentos anuais para disseminação da cultura de riscos e controles, em que se busca uma evolução contínua da gestão de riscos para todos os níveis da organização.

6. ATRIBUIÇÃO E RESPONSABILIDADE

A responsabilidade da gestão dos riscos permeia toda a organização e requer a participação ativa de todas as áreas da Companhia. Para cada estrutura de gestão, são estabelecidas atribuições e responsabilidades considerando a extensão de suas competências na atuação conjunta com os órgãos de governança corporativa. A estes órgãos, são atribuídas as seguintes responsabilidades específicas:

6.1. Conselho de Administração

a) Estabelecer as diretrizes gerais das estratégias de Gestão de Riscos;

b) Definir e revisar periodicamente o apetite a riscos da organização;

c) Aprovar a Política de Gerenciamento de Riscos e suas revisões futuras;

d) Avaliar se a estrutura de Gestão de Riscos (pessoas e processos) está adequada e tem recursos suficientes;

e) Avaliar o nível de efetividade do sistema de controles internos da organização, como também, fornecer orientações para o seu aprimoramento constante;

f) Monitorar de forma contínua os riscos que podem impactar os objetivos da organização por meio de aprovação dos relatórios de acompanhamento;

g) Patrocinar a cultura de gestão de riscos com apoio da Diretoria e do Comitê de Auditoria e Riscos, o qual assumirá a liderança no acompanhamento do cumprimento dessa Política de Gestão de Riscos.

6.2. Comitê de Auditoria e Riscos

a) Supervisionar a adequação dos processos relativos ao gerenciamento de riscos e ao sistema de controles internos de acordo com as diretrizes estabelecidas pelo Conselho de Administração;
b) Monitorar a execução dos planos de ação para o tratamento dos riscos, prazos e seus respectivos responsáveis;
c) Avaliar a adequação dos recursos atribuídos ao processo de gestão dos riscos;
d) Manter o Conselho de Administração devidamente informado sobre a eficácia dos processos de gestão dos riscos;
e) Recomendar ao Conselho de Administração a correção ou aprimoramento de políticas, práticas e procedimentos identificados, como também, informar a necessidade de alterações nos níveis de apetite ao risco.

6.3. Diretoria

No funcionamento do sistema de governança de *Compliance*, a Diretoria é responsável por:

a) Cumprir a Política de Gestão de Riscos e, sempre que necessário, propor ao Conselho de Administração eventuais aperfeiçoamentos ou revisões;

b) Identificar riscos preventivamente e fazer sua respectiva gestão, avaliando a probabilidade de sua ocorrência e adotando medidas para sua prevenção e/ou mitigação;

c) Comunicar tempestivamente à área de Gestão de Riscos sobre riscos não identificados;

d) Garantir os recursos necessários para a implementação de controles internos efetivos e estratégias de mitigação dos riscos;

e) Validar as revisões periódicas do mapeamento dos Riscos com impacto nas estratégias.

6.4. Área de Gestão de Riscos

a) Manter atualizadas a política, a estrutura e a metodologia para que as áreas de negócio possam identificar, analisar e, efetivamente, gerenciar seus riscos visando o cumprimento dos objetivos;

b) Apoiar os gestores utilizando os conceitos e abordagens da metodologia utilizada na gestão do risco corporativo que os classifica de acordo com a gravidade dos seus potenciais impactos;

c) Avaliar a efetividade dos controles internos, indicadores e o nível de conformidade dos processos;

d) Monitorar o desenvolvimento, a implementação e o desempenho da estrutura do gerenciamento de riscos, incluindo o seu aperfeiçoamento;

e) Recomendar mecanismos de controle e planos de ação para mitigação dos riscos identificados para redução da probabilidade de eventos de risco e/ou mitigação de suas consequências;

f) Promover a disseminação da cultura de gerenciamento de riscos por meio de conscientização sobre a importância da gestão de riscos e a responsabilidade inerente a cada colaborador;

g) Consolidar a avaliação de riscos por meio da elaboração de relatórios periódicos e reportá-los às estruturas de governança.

6.5. Área de Auditoria Interna

a) Monitorar periodicamente as ações de mitigação dos riscos e as fragilidades registadas nos relatórios de auditoria, além de alimentar o modelo de gestão dos riscos com informações;

b) Assessorar o Conselho de Administração, informando e recomendando melhorias de adequação no ambiente interno e efetividade no processo de Gestão de Risco;

c) Identificar riscos que possam não ter sido mapeados no processo de gestão de riscos, através de uma avaliação independente do ambiente dos controles internos.

6.6. *Risk Owners*

a) Identificar e avaliar os riscos nos processos e nos negócios sob sua responsabilidade, aplicando as diretrizes estabelecidas nesta política;

b) Implementar controles internos e acompanhar as ações corretivas e/ou preventivas em sua área;

c) Assegurar a eficácia dos controles internos utilizados para mitigar os riscos;

d) Comunicar à área de Gestão de Riscos qualquer deficiência ou inadequação de processos internos/controles (pessoas e sistemas), ou de eventos externos;

e) Garantir a integridade das informações fornecidas à área de Gestão de Riscos.

7. VIGÊNCIA

Esta Política entra em vigor na data de aprovação pelo Conselho de Administração, revogando-se disposições em contrário.

8. SANÇÕES

A inobservância desta política poderá acarretar medidas disciplinares, até e inclusive a demissão, rescisão ou não renovação de contrato de trabalho e/ou medidas destinadas ao afastamento de membro do Conselho de Administração.

9. ATUALIZAÇÕES DESTA POLÍTICA

Esta Política poderá ser alterada, sempre que necessário, por deliberação da maioria dos membros do Conselho de Administração presentes à reunião que deliberar sobre o assunto. O controle das atualizações, revisões e aprovações do manual de processo a serem preenchidos sempre que julgado necessário.

CONTROLE DE VERSÕES E ALTERAÇÕES				
Versão	**Data**	**Responsável**	**Tipo de Alteração**	**Revisor/Aprovador**
01	**21.01.2020**	**Jurídico**	**Criação**	**Conselho de Administração**
02	**09.08.2022**	**Gestão de Risco**	**Atualização**	**Conselho de Administração**

ANEXO I – DICIONÁRIO DE RISCOS

ESTRATÉGICO							CONFORMIDADE		
Governança			Político e Econômico	Gestão e Modelo do Negócio			Regulamentos e Legislações		Normas e Diretrizes Internas
Compliance	Reputação e imagem	Estrutura organizacional	Cenário Macroeconômico	Relacionamento com Clientes	Planejamento e controle	Landbanks	Ambiental	Trabalhista	Aderência as Regras
Conduta Antiética, Corrupção e Fraude	Investidores	Transação com partes relacionadas		Inovação	Concorrência	Sustentabilidade	Tributário	Cível	

OPERACIONAL				FINANCEIRO		
Pessoas	Fornecimento	Operação	Tecnologia da Informação	Crédito	Mercado	Liquidez
Retenção e Capacitação	Materiais e serviços	Qualidade do Produto	Segurança da informação	Inadimplência	Taxa de juros	Fluxo de Caixa
Dependência de Pessoas	Dependência ou Concentração	Saúde e Segurança no Trabalho	Infraestrutura	Concentração		
	Obrigações contratuais e terceirização	Capacidade e eficiência	Integridade das informações			
		Práticas Comerciais				