

POLÍTICA DE GERENCIAMENTO DE RISCOS DA VULCABRAS S/A

Índice

1. OBJETIVO	2
2. ABRANGÊNCIA	2
3. DEFINIÇÕES	2
4. DIRETRIZES	3
5. METODOLOGIA PARA AVALIAÇÃO DOS RISCOS E CONTROLES INTERNOS	3
6. ETAPAS DO GERENCIAMENTO DE RISCOS	4
7. IDENTIFICAÇÃO DOS RISCOS	5
8. AVALIAÇÃO DE RISCOS	5
8.1. O que é Risco	5
8.2. Risco Inerente	6
8.3. Risco Residual	6
8.4. Matriz de Riscos	7
8.5. Controle de Riscos	7
8.6. Monitoramento de Riscos	8
8.7. Report	8
9. RESPONSABILIDADES	9
10. DISPOSIÇÕES GERAIS	12

1 Objetivo

Esta Política de Gerenciamento de Riscos (“**Política**”) tem por objetivo definir as diretrizes a serem observadas para identificação, avaliação, controle e monitoramento contínuo dos riscos da Vulcabras S/A. (“Companhia”), visando ao fortalecimento do ambiente de governança corporativa, à aderência dos Controles Internos e aos normativos vigentes.

2 Abrangência

Esta política é de caráter institucional, aplicando-se, portanto, aos conselheiros, diretores e a todos os empregados da Companhia (“Colaboradores”) e das empresas integrantes do seu Grupo Econômico.

3 Definições

Para fins de interpretação desta Política, os termos e expressões listados a seguir, no singular ou no plural, terão os significados abaixo.

Apetite ao Risco: será definido a cada acontecimento de Risco ocorrido.

Área de Compliance: conjunto de áreas responsáveis por funções de compliance que, conforme previsão contida no Regulamento do Novo Mercado, poderão ser exercidas por áreas não operacionais, entre outras, as desenvolvidas pelas áreas jurídica, de controladoria, de auditoria interna e de relações com investidores.

Controle Interno: consiste em um processo desenvolvido para garantir, com razoável certeza, que sejam atingidos os objetivos da Companhia.

Evento: a ocorrência da não conformidade, materialização do risco.

Gerenciamento de Riscos: é o processo conduzido pela administração, gerências e colaboradores da Companhia, formulado para identificar eventos capazes de afetar os negócios da Companhia, e administrar os Riscos identificados de modo a mantê-los compatíveis com o Apetite ao Risco.

Órgãos de Governança: Conselho de Administração, Diretoria Estatutária e Comitê de Auditoria.

Processos/Projetos: conjunto de tarefas ou atividades desempenhadas pelas áreas e departamentos da Companhia.

Proprietários dos Riscos: Colaboradores da Companhia e das empresas integrantes de seu Grupo Econômico que possuem o maior domínio e conhecimento técnico acerca do Risco correspondente, responsável pela tomada de decisão e capaz de estabelecer e gerir os planos de ação.

Risco: é a probabilidade de perda ou a incerteza associada ao cumprimento de um objetivo, sendo inerente a qualquer atividade.

4 Diretrizes

4.1 Considerando que o Risco é inerente a qualquer atividade, função ou decisão, sejam elas internas ou externas ao ambiente organizacional, para que o processo de Gerenciamento de Riscos seja eficiente é necessário que haja na Companhia:

(i) Vontade dos Colaboradores em administrar Riscos;

(ii) Cultura corporativa que defina as responsabilidades (alçadas) de cada Colaborador na execução das suas atividades;

(iii) Estímulo ao levantamento de questões passíveis de serem avaliadas como arriscadas; e,

(iv) Definição objetiva da participação de cada Colaborador no controle de Riscos da sua respectiva área.

4.2. Os Riscos devem ser continuamente identificados, avaliados, controlados e monitorados. Devem ser identificados e avaliados quanto à sua frequência (probabilidade) e quanto à sua consequência (impacto) nos objetivos e metas estabelecidos pela Companhia.

5 Metodologia para Avaliação dos Riscos e Controles Internos

5.1 A Companhia adotará, mas não se limitará, a metodologia **CSA – Control Self-Assessment** para análise e revisão dos Riscos envolvidos na busca pelo alcance dos seus objetivos e dos Controles Internos.

5.2 A metodologia da autoavaliação “*Control Self Assessment – CSA*”, adotada pela Companhia, decorre da execução de algumas etapas que serão conduzidas pela Área de *Compliance*, com a participação dos gestores dos Processos, permitindo avaliar o ambiente de Riscos, os Controles Internos e a eficiência no gerenciamento destes, buscando melhorar o desempenho por meio de revisão de Processos e/ou da elaboração de planos de ação para melhorias.

5.3 Além disso, a Companhia realizará reuniões para avaliação dos Riscos e Controles Internos. Essas reuniões serão conduzidas pela Área de *Compliance*, em que também participarão os gestores do Processo e demais áreas envolvidas, e serão utilizados questionários para autoanálise dos gestores. O resultado do trabalho possibilitará a avaliação da eficiência dos controles e do Gerenciamento dos Riscos, buscando melhorar o desempenho por meio de revisão de processos, elaboração de plano de ação e criação de ferramentas para tratamento dos Riscos.

5.4 Sempre que necessário, deverão ser realizados ciclos de autoavaliação da Companhia e suas controladas, cujos resultados deverão ser avaliados pela Área de *Compliance* e levados a conhecimento do Conselho de Administração, Diretoria Estatutária e Comitê de Auditoria.

5.5 O acompanhamento do plano de ação resultante da autoavaliação deverá ser realizado pela Área de *Compliance*, juntamente com a emissão dos relatórios de Controles Internos, que possam subsidiar as decisões do Conselho de Administração e da Diretoria Estatutária da Companhia.

5.6 O ciclo de autoavaliação deverá ser realizado considerando os objetivos e metas, bem como as ações definidas no planejamento estratégico da Companhia.

5.7 Será elaborado um Plano de Ação para início das atividades, que defina as prioridades e o cronograma das atividades de mapeamento e monitoramento do ciclo de autoavaliação, e que contenha em seus anexos os formulários para apresentação dos Riscos identificados pelos gestores dos processos e projetos.

6 Etapas do Gerenciamento de Riscos

6.1 O processo de gestão de Riscos deverá ser realizado observando-se as seguintes etapas: i) identificação dos Riscos; ii) avaliação dos Riscos; iii) controle dos Riscos; iv) monitoramento dos Riscos e v) reporte, conforme especificação a seguir

7 Identificação dos Riscos

7.1 A identificação dos Riscos tem o objetivo de reconhecer e descrever os Riscos aos quais a Companhia está exposta, devendo ser realizada com a participação de todas as áreas e de todos os níveis hierárquicos envolvidos nos processos.

7.2 Os Riscos a serem identificados e avaliados são:

(i) **Risco Operacional:** Possibilidade de ocorrência de perdas decorrentes da inadequação na especificação ou na condução de processos, falhas em sistemas ou projetos da Companhia, bem como de eventos externos que causem prejuízos na execução de suas atividades normais ou danos a seus ativos físicos.

(ii) **Risco de Imagem:** Possibilidade de ocorrência de perdas financeiras, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas, por pessoas não autorizadas ou por meios de comunicação inadequados; e por veiculação de notícias negativas sobre a Companhia ou seu segmento.

(iii) **Risco Reputacional:** pode ser representado por todos os eventos internos e externos com capacidade de manchar ou danificar a percepção da Companhia perante a mídia, o público, os colaboradores e o mercado em geral.

(iv) **Risco Financeiro:** Os Riscos financeiros, em definição, são todas as possibilidades (variantes) que podem levar a Companhia a perder dinheiro, seja através de transações financeiras, erros de execução de processos, investimentos, dentre outros.

(v) **Risco Regulatório /Ambiental/ Legal / Tributário:** São os Riscos relacionados à possibilidade de impacto causado por uma eventual mudança na legislação vigente ou normas regulamentadoras, ou pelo descumprimento ou falta de habilidade em cumprir com a legislação ou regulamentação aplicáveis.

8 Avaliação de Riscos

8.1 A avaliação de Riscos consiste em comparar os resultados da análise de Riscos com os critérios de Riscos para determinar se o Risco é aceitável. Isto envolve avaliar o nível de Risco a fim de subsidiar a tomada de decisão e determinar a ordem de prioridade de tratamento dos Riscos.

8.1.1. A análise de Risco é o processo pelo qual os gestores da Companhia avaliam a probabilidade real de acontecerem determinados eventos negativos, imprevistos e incertezas decorrentes ou durante determinada ação. Em sua análise deverá considerar a complexidade dos Riscos e as informações disponíveis para sua avaliação, podendo ser realizada por meio de análises qualitativas, quantitativas ou semiquantitativas, visando à definição do impacto e da frequência de cada Risco.

8.1.2. A **análise qualitativa** consiste na utilização de descrições de palavras e escalas, para mensuração das consequências de um determinado Risco e da probabilidade de sua ocorrência.

8.1.3. A **análise quantitativa** utiliza apenas valores numéricos para mensurar a amplitude do impacto e da frequência da ocorrência dos Riscos.

8.1.4. A **análise semiquantitativa** consiste na combinação das análises qualitativa e quantitativa, que por sua vez proporciona duas vantagens: i) menor complexidade e custo operacional quando comparado com o método quantitativo; e ii) maior grau de objetividade quando comparado com o método qualitativo.

8.1.5. Considerando a fase de estruturação da Companhia e a indisponibilidade de séries históricas de dados relacionados com inúmeros eventos de Riscos associados às atividades da Companhia, os ciclos de análises de Riscos serão, sempre que possível, baseados em análises semiquantitativas.

8.1.6. A probabilidade e impacto do Risco e suas consequências deverão ser analisados pelas perdas monetárias ou de credibilidade, que podem ser causados para a Companhia, conforme explicado a seguir:

8.2. Risco Inerente

8.2.1. Risco inerente é o Risco que se origina na natureza da própria operação/negócio. Está intrínseco à operação/negócio, à atividade desenvolvida.

8.2.2. É a hipótese inicial de ocorrência de irregularidades, anomalias, equívocos ou mesmo grandes erros que podem comprometer uma atividade.

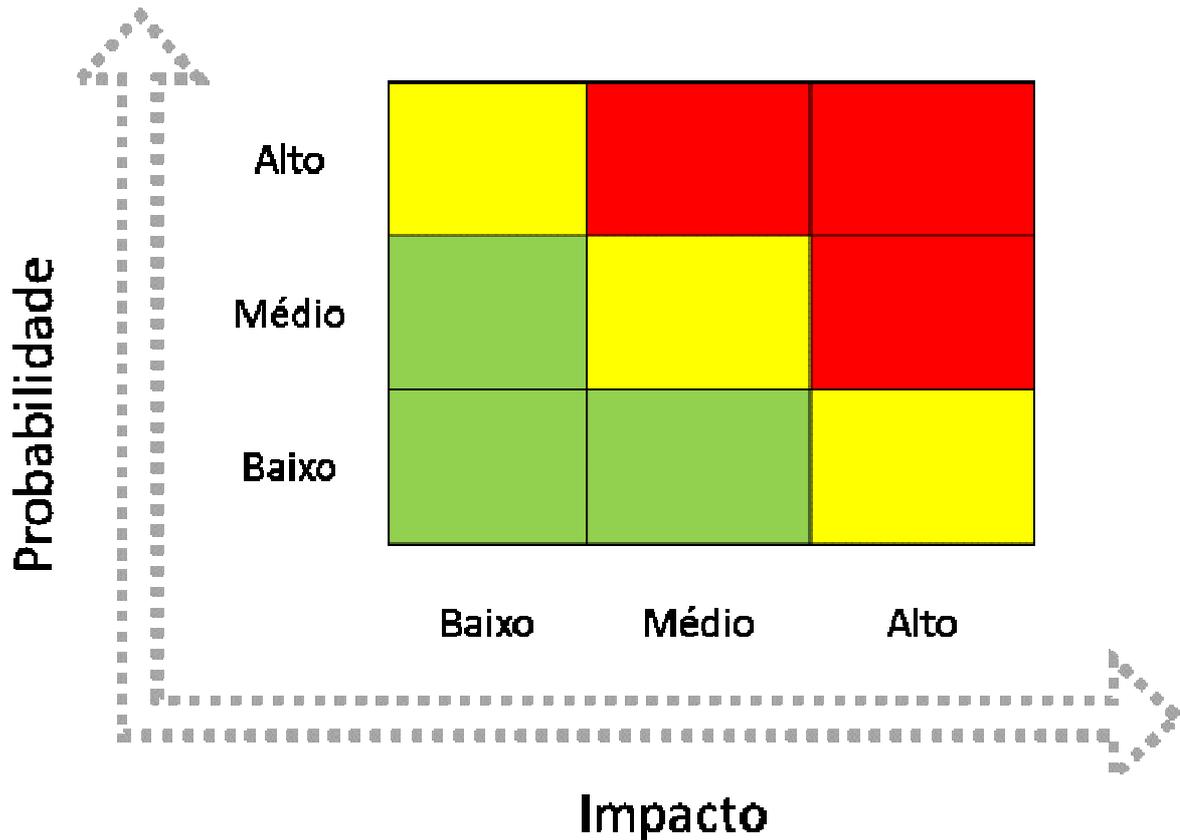
8.2.3. Precisa ser conhecido para que se saiba a consequência real caso venha a ocorrer falha nos controles.

8.3 Risco Residual

8.3.1. É o Risco que permanece após a gestão tomar ações para reduzir o impacto e probabilidade de um evento adverso, incluindo as atividades de controle para responder a um Risco.

8.4. Matriz de Riscos

8.4.1. Os Riscos identificados e avaliados deverão ser registrados em uma matriz de Riscos, conforme escala a seguir:



8.5 Controle de Riscos

8.5.1. Posteriormente à etapa de avaliação dos Riscos, deverá ser definida a resposta que será dado aos Riscos.

8.5.2. Tratar os Riscos consiste em decidir entre evitá-los, mitigá-los, compartilhá-los ou aceitá-los. A decisão dos gestores depende, principalmente, do grau de Apetite ao Risco da Companhia, previamente definido e aprovado pelo Conselho de Administração e Diretoria Estatutária.

- **Evitar o Risco:** consiste na eliminação total do Risco, decidindo-se por descontinuar a atividade que seja fonte do Risco. É necessário avaliar se, evitando-se um Risco, tal decisão não aumentaria a possibilidade de outro Risco ocorrer.

- **Mitigar o Risco:** consiste em implementar ou aprimorar atividades de controles, com o objetivo de reduzir o impacto e a frequência da ocorrência do Risco, onde seu benefício deverá ser maior do que seu custo. (Ex: trabalhos de revisão criteriosa, *check-list* das atividades, contratação de sistemas informatizados, segregação de funções, etc).
- **Compartilhar o Risco:** consiste em compartilhar com outras partes os impactos provocados pelo Risco, geralmente buscando a reparação das perdas, reduzindo o Risco a um nível compatível com as tolerâncias aceitáveis pela Companhia.
- **Assumir o Risco:** significa que identificado e registrado no seu plano de gerenciamento de Riscos, você não vai tomar nenhuma ação. Simplesmente você aceita que ele possa acontecer e decidirá como lidar com ele caso ocorra.
- **Transferir o Risco:** transferir o Risco para um terceiro, ou para outra área de negócio que seja responsável pelo processo em que o Risco é originado.

8.5.3. Ao determinar respostas a Riscos, a Companhia deverá levar em conta os efeitos do impacto da ocorrência do Risco e que opções de resposta são compatíveis com as tolerâncias a Risco da Companhia, os custos *versus* os benefícios do tratamento e as possíveis oportunidades da Companhia em alcançar seus objetivos.

8.6 Monitoramento de Riscos

8.6.1. Visando ao aprimoramento contínuo da gestão de Riscos, o processo de monitoramento consiste em acompanhar o desempenho dos indicadores de gestão, supervisionar a implantação e manutenção dos planos de ação, o alcance das metas estabelecidas para a Companhia e a eficácia e eficiência dos Controles Internos.

8.6.2. Os resultados da identificação e avaliação dos Riscos e dos Controles Internos, decorrentes dos ciclos de autoavaliação, serão registrados em relatórios específicos, que subsidiarão a emissão da manifestação do Conselho de Administração e Diretoria Estatutária da Companhia.

8.6.3. Os Proprietários dos Riscos deverão manter atualizados os relatórios que contemplem o resultado dos monitoramentos dos Riscos decorrentes das recomendações e dos planos de ação identificados nos relatórios da Área de *Compliance*.

8.7 Reporte

8.7.1. As informações pertinentes são identificadas, coletadas e comunicadas de forma coerente e no prazo, a fim de permitir que as pessoas cumpram as suas responsabilidades.

9 RESPONSABILIDADES

9.1 A Companhia entende que para alcançar os seus objetivos está exposta aos Riscos descritos nesta Política, que devem ser gerenciados por cada área, a comando do seu respectivo líder. As três linhas de defesa consistem em um conceito que define os papéis e responsabilidades no gerenciamento de Riscos e Controles Internos e fortalecimento da governança, bem como a interação desses papéis em todos os níveis da Companhia, conforme indicado abaixo:

9.2. **1ª Linha de Defesa:** é representada pelas Proprietários dos Riscos, cujos colaboradores são os responsáveis diretos pela gestão dos Riscos e pela aderência às normas associadas às suas atividades, bem como pela execução dos Controles Internos e pela implementação de medidas corretivas para o devido tratamento dos Riscos.

9.3. **2ª Linha de Defesa:** é representada pela Área de Compliance, responsável pelas funções de compliance, riscos e Controles Internos da Companhia, que atua na garantia do apropriado funcionamento da primeira linha, por meio do estabelecimento de controles, na identificação de falhas de performance de controles e na identificação de desvios de políticas e procedimentos internos. As atividades da Área de Compliance são acompanhadas pelo Comitê de Auditoria e reportadas para o Conselho de Administração, por meio da Diretoria.

9.4. **3ª Linha de Defesa:** é representada pela Auditoria Interna que atua no fornecimento de avaliações independentes à administração, por meio de técnicas de auditoria. Permite à administração aferir a adequação dos controles, a efetividade do Gerenciamento dos Riscos e o cumprimento das normas e regulamentações. A Auditoria Interna tem suas atividades reportadas periodicamente ao Conselho de Administração da Companhia, por meio do Comitê de Auditoria, e suas atribuições são aprovadas pelo Conselho de Administração da Companhia.

9.5. Neste sentido, o gerenciamento de Riscos da Companhia está estruturado conforme organograma e descrições abaixo, sem prejuízo das demais disposições desta Política.



9.6. Compete ao **Conselho de Administração**, no âmbito desta Política:

- (i) definir os objetivos estratégicos, as diretrizes e o *Apetite de Riscos* da Companhia, adequado e aderente aos seus negócios;
- (ii) aprovar as políticas, diretrizes, limites de exposição e impactos propostos;
- (iii) regular a priorização dos Riscos a serem tratados
- (iv) avaliar mudanças ou atualizações de Riscos cujos limites já tenham sido aprovados;

9.7. Compete ao **Comitê de Auditoria** da Companhia, órgão autônomo de assessoramento vinculado ao Conselho de Administração, no âmbito desta Política:

- (i) monitorar o cumprimento desta Política e avaliar a performance frente aos limites de Risco aprovados;
- (ii) avaliar a efetividade do modelo de gestão de Riscos e sugerir aprimoramentos no processo, apontando as causas e responsabilidades; e
- (iii) certificar que a área de Auditoria Interna esteja adotando todas as providências previstas no item 10.6, abaixo, além das atribuições que lhe são próprias.

9.8. Compete à Diretoria Estatutária, no âmbito desta Política da Companhia:

- (i) estabelecer priorização dos Riscos a partir do impacto e probabilidade, visando estabelecer uma comparação individual dos Riscos;
- (ii) avaliar e tomar decisões em relação a exposição aos Riscos (impacto e probabilidade) e recomendar ações de respostas;
- (iii) acompanhar periodicamente a evolução da exposição aos Riscos considerando os limites aprovados pelo Conselho de Administração;
- (iv) disseminar a cultura de gerenciamento de Risco em toda Companhia.

9.9. Compete à área de **Auditoria Interna**, no âmbito desta Política:

- (i) aferir a qualidade e a efetividade do processo de gerenciamento de Riscos e dos processos de governança, da adequação dos controles e do cumprimento das normas e regulamentos associados aos negócios da Companhia, de forma independente, imparcial e tempestiva; e
- (ii) fornecer relatórios periódicos ao Comitê de Auditoria, a fim de garantir que os processos e estrutura de Gerenciamento de Riscos esteja sendo devidamente obedecida.

9.10 Compete à **Área de Compliance**, no âmbito desta Política:

- (i) apoiar a primeira linha de defesa na observação de suas responsabilidades diretas;
- (ii) orientar e aconselhar os colaboradores da Companhia, direcionando soluções específicas sobre o cumprimento desta Política;
- (iii) categorizar os Riscos conforme sua prioridade e monitorar a exposição da Companhia a esses Riscos;
- (iv) certificar a eficiência do ambiente de gerenciamento de Riscos e Controles Internos;
- (v) revisar e acompanhar os planos de ação;
- (vi) informar à Diretoria, ao Comitê de Auditoria e reportar ao Conselho de Administração as situações relevantes e que não estejam em conformidade;
- (vii) elaborar relatórios de reporte ao Conselho de Administração e ao Comitê de Auditoria, consolidando a avaliação de Riscos da Companhia;
- (viii) estabelecer os processos de Gerenciamento de Riscos;

- (ix) monitorar o sistema de gestão de Riscos, reportando as atividades de gestão de Riscos ao Comitê de Auditoria, e indiretamente ao Conselho de Administração;
- (x) zelar pela aplicação do Código de Ética e Conduta da Companhia e das demais políticas de integridades;
- (xi) Conduzir reuniões para avaliação dos Riscos e Controles Internos e os ciclos de autoavaliação e levar os resultados para conhecimento do Conselho de Administração, da Diretoria Estatutária e do Comitê de Auditoria;
- (xii) elaborar o plano de implantação dos procedimentos e diretrizes do Código de Ética Conduta, bem como das demais políticas de integridades;

9.11. Compete aos Proprietários dos Riscos da Companhia:

- (i) identificar, mensurar e gerenciar os fatores de Risco que possam influenciar o cumprimento dos objetivos estratégicos e operacionais da Companhia;
- (ii) manter um efetivo ambiente de gerenciamento de Riscos e Controles Internos, consistente com a natureza, o porte, a complexidade, a estrutura, o perfil de Risco e o modelo de negócio das operações realizadas, de forma a assegurar o efetivo gerenciamento dos Riscos, mantendo a exposição aos Riscos em níveis aceitáveis;
- (iii) manter a conformidade com as normas e exigências regulatórias;
- (iv) fornecer informações precisas, íntegras e suficientes para análises;
- (v) comunicar, tempestivamente, os eventos de Risco que apresentarem tendência de ocorrência e/ou eventual extrapolação de limites, para discussão nos fóruns e alçadas apropriadas;
- (vi) cumprir os limites de Riscos aprovados pelo Conselho de Administração;
- (vii) dar cumprimento ao plano de ação; e
- (viii) reportar continuamente à área de Compliance e/ou à Auditoria Interna, conforme o caso, todos os fatores de Risco e/ou eventos que possam impactar e/ou interferir, direta ou indiretamente, no mapeamento dos riscos da Companhia.

10 DISPOSIÇÕES GERAIS

10.1. A Companhia se reserva ao direito de, a qualquer momento, revisar, modificar, alterar ou revogar esta Política, especialmente no caso de qualquer alteração essencial ou relevante nas leis ou nos regulamentos aplicáveis à Companhia, por deliberação do Conselho de Administração.

10.2. No caso de conflito entre as disposições desta Política e do Estatuto Social, prevalecerá o disposto no Estatuto Social e, em caso de conflito entre as disposições desta Política e da legislação vigente, prevalecerá o disposto na legislação vigente.

10.3. Caso qualquer disposição desta Política venha a ser considerada inválida, ilegal ou ineficaz, essa disposição será limitada, na medida do possível, para que a validade, legalidade e eficácia das disposições remanescentes desta Política não sejam afetadas ou prejudicadas.

10.4. Os casos omissos serão decididos pelo Conselho de Administração da Companhia.

10.5. A presente Política entra em vigor na data de sua aprovação pelo Conselho de Administração, vigendo por prazo indeterminado, e será publicado no website de Relações com Investidores da Companhia e divulgado na forma prevista na legislação e regulamentação aplicável.

A presente Política foi aprovada em 06 de abril de 2022 pelo Conselho de Administração.