POLÍTICA
DE GERENCIAMENTO DE RISCOS
PETRO RIO S.A.

Índice

1. Objetivo

O objetivo desta Política de Gerenciamento de Riscos ("Política") é estabelecer princípios, diretrizes e responsabilidades que devem ser observados no processo de Gerenciamento de Riscos Corporativos inerentes às atividades da PetroRio, a partir da identificação, análise, priorização, abordagem de tratamento, monitoramento e a comunicação dos riscos que podem afetar o alcance e a execução da estratégia planejada.

Adequando a governança da empresa às boas práticas de mercado, o processo de tomada de decisões se torna mais robusto, incorporando a visão de riscos corporativos, o que possibilita a criação e preservação de valor para a PetroRio.

Ademais, a política visa ser um instrumento para auxiliar na disseminação da cultura de gestão de riscos corporativos pela PetroRio, na medida em que busca estabelecer uma linguagem comum acerca do tema, bem como determinar as responsabilidades de cada agente de governança envolvido no processo.

2. Abrangência

Esta Política se aplica a todos os conselheiros, diretores, colaboradores, terceiros, e a todas as pessoas que trabalham direta ou indiretamente para a PetroRio, suas subsidiárias, empresas sob controle comum, consorciadas, parceiros de negócios e comerciais com os quais a PetroRio possua relacionamento de negócios, independentemente da natureza da relação, se continuada ou pontual, se envolve a transferência de recursos financeiros ou apenas de conhecimento (know-how). Destaca-se que a política passará também a se aplicar automaticamente a novas empresas controladas e coligadas.

3. Definições

- **Ação mitigatória**: Ações e controles implementados pela PetroRio com o objetivo de mitigar a exposição ao risco, reduzindo a probabilidade de materialização do mesmo;
- **Apetite a Risco**: Nível de risco que a PetroRio está disposta a aceitar na busca e realização de sua estratégia e objetivos. Destaca-se que nem todos os tipos de risco são passíveis de aceitação;
- **Enterprise Risk Management (ERM) / Gestão de Riscos Corporativos**: Processo conduzido pelas diferentes instâncias de governança da empresa, como Conselho de Administração, Comitê de Ética e Compliance e áreas de negócio, que visa estabelecer estratégias para identificar, analisar, avaliar, tratar, monitorar e comunicar potenciais eventos que possam afetar a execução da estratégia planejada;
- **Fator de Risco Corporativo**: Situações e/ou circunstâncias que podem levar ao aumento da probabilidade de ocorrência de um risco;
- ***Key Risk Indicator* (KRI) / Indicador-chave de risco**: Métrica utilizada para obter a exposição ao risco corporativo, sendo recomendado que esteja relacionado à causa do risco e aferido de forma em periodicidade definida conforme criticidade do fator, visando antecipar uma possível materialização do risco;
- **Impacto**: São as consequências em decorrência da materialização de um risco corporativo, que pode ser expresso de forma quantitativa e/ou qualitativa;
- **Mapa de Riscos Corporativos**: Representação gráfica dos riscos corporativos alocados de acordo com a criticidade de cada risco por meio da avaliação de seu impacto e de sua probabilidade;
- **Plano de ação**: Plano contendo as ações a serem implementadas pela PetroRio visando mitigar o risco identificado;

- **Portfólio de Riscos Corporativos**: Catálogo contendo a relação de riscos corporativos e seus respectivos fatores de risco;
- **Probabilidade**: Chance do risco corporativo se materializar;
- **Proprietário do Risco**: Colaborador da PetroRio responsável pelas ações de mitigação e monitoramento do risco corporativo que está sob sua competência;
- **Régua de Impacto x Probabilidade**: Documento que formaliza o descritivo e os critérios a serem considerados para cada uma das dimensões analisadas na classificação do nível de Impacto e Probabilidade dos riscos corporativos identificados, resultando na indicação do risco Inerente e Residual;
- **Resposta ao Risco**: Definição do tratamento que a PetroRio atribuirá ao fator de risco. Como resposta, pode-se optar por evitar, reduzir, compartilhar ou aceitar;
- **Risco**: Possibilidade de ocorrência de um evento que tenha impacto adverso, dificultando ou impossibilitando o atingimento dos objetivos estratégicos da PetroRio;
- **Risco Corporativo**: Riscos que possam impactar no alcance e execução da estratégia planejada ou o negócio como um todo;
- **Risco Inerente**: Risco intrínseco a operação do negócio ou à atividade, não sendo considerado as ações e os controles existentes na empresa;
- **Risco Residual**: Risco remanescente após considerar todas as ações e controles existentes para mitigá-lo.

4. Diretrizes

4.1 Para o gerenciamento de riscos corporativos

A PetroRio está comprometida com o Gerenciamento de Riscos e tem como prática a análise constante dos riscos aos quais está exposta e que possam afetar seus negócios, situação financeira e os resultados das suas operações de forma adversa.

Neste sentido, o modelo de gerenciamento de riscos praticado na PetroRio tem como base o conceito de três linhas do Instituto dos Auditores Internos (IIA), onde cada ente da organização tem papéis definidos em seu processo de gestão dos riscos. Conforme estabelecido, o modelo “ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos”.

Fonte: Declaração de Posicionamento do Institute of Internal Auditors (IIA) – as três linhas no gerenciamento eficaz de riscos e controles (2020).

Tal modelo prevê as seguintes atribuições a cada instância:

- **Corpo Administrativo**: Composto pela direção da PetroRio, são os responsáveis perante os stakeholders pelo sucesso da organização, assegurando que os objetivos e atividades organizacionais estejam alinhados aos interesses priorizados dos stakeholders;
- **1ª Linha**: Funções/ áreas que gerenciam e têm propriedade sobre os riscos - incluem tanto atividades de "*front of house*" quanto de "*back office*", são as áreas responsáveis por manter os controles internos eficazes, conduzindo no seu dia-a-dia os procedimentos de gerenciamento de riscos e controles.
- **2ª Linha**: Funções/ áreas que supervisionam riscos - representada por áreas de suporte / conhecimento técnico, são aquelas responsáveis por estabelecer as diretrizes e procedimentos relacionados ao gerenciamento de riscos e conformidade para o desenvolvimento e/ou monitoramento dos controles da primeira linha.
- **3ª Linha**: Funções que fornecem análise/avaliações independentes - A Auditoria Interna é uma atividade independente e objetiva de avaliação e de consultoria desenhada para adicionar valor e melhorar as operações de uma organização. Neste conceito, é responsável pela revisão independente do gerenciamento dos riscos, suportando a organização no atingimento de seus objetivos e apresentando uma abordagem sistemática e disciplinada para avaliar e aperfeiçoar a eficácia dos processos de gestão de riscos, controles e governança.

4.2 Para a identificação dos riscos

Esta etapa visa identificar e mapear os riscos aos quais a PetroRio possa estar exposta e que possam afetar a sua estratégia, objetivos e operação. Ou seja, a identificação dos riscos envolve descrever os riscos aos

quais a Companhia está exposta, definindo sua natureza e as causas, consequências e os responsáveis por cada risco.

O mapeamento dos riscos requer o envolvimento das três linhas, podendo ser realizados por meio de entrevistas com os principais executivos e gestores da empresa, pesquisas de percepção aplicadas, análises documentais provenientes de avaliações realizadas, relatórios e/ou cartas de controles internos emitidos por auditorias internas e/ou externas, incluindo fiscalizações, dentre outros. Dada a atuação da empresa, o mapeamento de riscos também poderá considerar fatores externos a organização, como: econômicos, políticos, sociais, ambientais, dentre outros.

Com base no referencial teórico proposto pelo COSO ERM bem como a cultura organizacional da empresa, e visando facilitar a avaliação, tratamento e monitoramento dos riscos, a PetroRio categorizou os seus riscos nas seguintes categorias dispostas em seu Portfólio de Riscos Corporativos:

- **Estratégico**: risco de perdas resultantes do insucesso das estratégias adotadas, levando-se em conta a dinâmica dos negócios e da concorrência, consecução da estratégia de fusões e aquisições, as alterações políticas e econômicas no País e fora dele, imagem da empresa, além de questões ambientais, sociais e de governança.
- **Financeiro**: risco de perdas resultantes de flutuações de mercado que impactem os ativos da organização, bem como os riscos relacionados à capacidade de crédito dos clientes e fontes pagadoras e a liquidez da PetroRio para com suas obrigações financeiras;
- **Operacional**: risco de perdas resultantes de falhas ocorridas nos processos e operações, gestão de terceiros, contratos, tecnologia da informação, além dos relacionados aos processos de Gente e Gestão.
- **Conformidade**: riscos de perdas e sanções legais ou regulatórias que a empresa possa vir a sofrer em decorrência de falha no cumprimento de regulamentos e legislações que possam vir a causar ou que causem prejuízo à reputação e imagem da PetroRio.

4.3 Para a avaliação dos riscos

Identificados os riscos, estes deverão ser avaliados no que tange as óticas de Impacto e Probabilidade, seja na indicação do risco Inerente, ou seja na indicação do risco Residual. Para tal, deverá ser considerada a **Régua de Impacto x Probabilidade** aprovada pelo Comitê de Ética e Compliance.

Mediante a análise dos controles existentes na PetroRio e seu referido grau de exposição, os riscos deverão ser priorizados com o intuito de possibilitar o foco adequado no tratamento dos riscos considerados de exposição elevada / superior ao apetite a risco definido.

Nesta etapa, a função de Controles Internos deverá ser envolvida para auxiliar na identificação dos controles internos existentes e/ou ausentes, visando assegurar o adequado endereçamento do risco residual. Para o endereçamento da substância do controle, e conforme entendimento do proprietário do risco e da materialidade do mesmo, serão aplicadas as técnicas da autoavaliação e/ou do walkthrough.

Ademais, recomenda-se que os controles internos sejam avaliados de forma independente pela Auditoria Interna em uma base periódica, com o intuito de ratificar e/ou retificar o grau de exposição a determinado evento de risco.

4.4 Para o tratamento dos riscos

Esta etapa envolve a definição, por parte da gestão, de uma resposta para os riscos identificados de modo a trazer a exposição a um determinado risco a um nível que seja aceitável para a PetroRio, conforme definido em seu apetite a riscos.

É possível optar por quatro respostas ao risco, sendo elas: aceitar, evitar, mitigar ou compartilhar

- **Aceitar o risco:** Nenhuma ação é tomada para o risco identificado. O risco é geralmente aceito quando seu nível está dentro das faixas de apetite de risco da PetroRio. Nessa situação, não há necessidade de um novo controle para mitigar o risco, pois os controles existentes têm sido aplicados de forma efetiva e contínua, podendo ser objeto de inspeção e/ou teste;
- **Evitar o risco:** Descontinuar as atividades que geram o risco. Um risco geralmente é evitado quando há probabilidade de um impacto significante nos objetivos da PetroRio e os custos de implantação de controles são muito elevados, dificultando sua mitigação; ou não é possível a sua transferência;
- **Mitigar o risco:** Implementar controles que reduzam as causas e efeitos do risco. Um risco geralmente é mitigado quando há probabilidade de um impacto significante nos objetivos da PetroRio. A implementação de controles, neste caso, apresenta um custo / benefício adequado;
- **Compartilhar o risco:** Reduzir o risco atribuindo-o a um terceiro por meio, por exemplo, da contratação de um seguro, adoção de instrumento de *hedge*, dentre outros. Um risco é compartilhado quando há probabilidade de um impacto significativo nos objetivos da PetroRio, mas a implementação de controles não apresenta um custo/benefício adequado.

4.5 Para a assunção dos riscos

Consiste na análise e validação pelo Proprietário do Risco, Comitê de Ética e Compliance e Diretoria Executiva do nível de exposição a um risco, considerando possíveis justificativas para tal (como não ser viável estabelecer ações para sua mitigação) e, assim, aceitando as consequências que essa situação poderá trazer futuramente.

Todos os processos de assunção de riscos deverão ser enviados para o conhecimento da Diretoria Executiva.

Criticidade do Risco	Alçada de Aceite	Alçada de Aprovação
Crítico e Significativo	Comitê de Ética e Compliance	Diretoria Executiva
Moderado	Proprietário do Risco	Comitê de Ética e Compliance
Baixo e Mínimo	Proprietário do Risco	

5. Responsabilidades

5.1 Conselho de Administração

- Aprovar a Política de Gestão de Riscos Corporativos, bem como suas alterações oriundas das revisões;
- Definir o perfil de risco da PetroRio;

- Avaliar a adequação da função de riscos de forma a assegurar a efetividade desta Política.
- Assegurar a efetividade e acompanhar o cumprimento do processo de Gerenciamento de Riscos da PetroRio;
- Assegurar a autoridade, autonomia, independência e responsabilidade da função de riscos;

5.2 Comitê de Ética e Compliance

- Validar e aprovar a Régua de Impacto e Probabilidade;
- Aprovar as diretrizes do processo de Gestão de Risco Corporativos, incluindo a matriz de riscos identificados;
- Assegurar o cumprimento da matriz de alçadas para a assunção dos riscos;
- Apoiar a disseminação da cultura de Gestão de Riscos;
- Avaliar a adequação dos recursos humanos e financeiros destinados à gestão de riscos corporativos;
- Acompanhar os planos de ação de tratamento dos riscos;
- Receber reporte da função de riscos para avaliar periodicamente a matriz dos riscos corporativos priorizados e ações mitigatórias estabelecidas;
- Assessorar o Conselho de Administração na avaliação e monitoramento periódico do portfólio de riscos corporativos.

5.3 Diretoria Executiva

- Participar do processo de Gestão de Riscos Corporativos e assegurar que esteja alinhado às práticas da PetroRio e às boas práticas de mercado;
- Assegurar a adequação dos recursos humanos e financeiros destinados à gestão de riscos corporativos;
- Disseminar a cultura da Gestão de Riscos para toda a PetroRio;
- Apreciar eventuais alterações nas disposições da Política de Gestão de Riscos Corporativos;
- Participar do processo de construção e atualização do portfólio de riscos corporativos;
- Contribuir com a avaliação dos riscos, conforme os critérios de impacto e probabilidade estabelecidos;
- Apoiar na definição dos proprietários dos riscos corporativos;
- Aprovar o portfólio e indicar os riscos a serem priorizados;
- Assegurar o *enforcement* para que os proprietários dos riscos atuem adequadamente na avaliação, tratamento e monitoramento dos riscos corporativos;
- Avaliar os planos de ação a serem capitaneados pelos proprietários dos riscos corporativos priorizados;
- Aprovar processo de assunção de responsabilidade relacionado aos riscos significativos e altos após o aceite do Comitê de Ética e Compliance.

5.4 Função de Riscos

- Desenvolver, sugerir e revisar diretrizes para o processo de gestão de riscos corporativos da PetroRio;
- Elaborar e manter atualizada a Política de Gestão de Riscos Corporativos;
- Acompanhar a implementação da Política de Gestão de Riscos Corporativos por toda a PetroRio;

- Elaborar e realizar o plano de trabalho, incluindo orçamento, recursos (humanos e tecnológicos) e prazos, a fim de viabilizar a execução do processo de Gestão de Riscos Corporativos de maneira eficiente;
- Auxiliar na adequação das áreas ao perfil de risco da PetroRio;
- Promover a interface entre o processo de gerenciamento de riscos e de atualização da estratégia de negócios;
- Desenvolver ações de comunicação e treinamento visando disseminar a cultura de Gestão de Riscos Corporativos por toda a PetroRio;
- Fornecer apoio metodológico para a gestão dos riscos corporativos às áreas da PetroRio;
- Receber e consolidar eventuais mudanças na criticidade dos riscos corporativos e reportá-las à Diretoria Executiva, Comitê de Compliance e ao Conselho de Administração;
- Monitorar e consolidar os status dos planos de ação e indicadores de risco (KRIs), enviados pelos proprietários dos riscos corporativos e emitir reportes periódicos à Diretoria Executiva, ao Comitê de Ética e Compliance e ao Conselho de Administração;
- Propor a revisão do portfólio de riscos corporativos sempre que houver atualizações no planejamento estratégico.

5.5 Função de Controles Internos

- Atuar no aprimoramento contínuo do ambiente de controles internos da PetroRio;
- Atuar em conjunto com a função de Gestão de Riscos no apoio aos proprietários de risco;
- Disseminar a cultura de controles internos na PetroRio por meio de treinamentos e comunicações direcionadas;
- Mapear os processos internos da PetroRio conforme o grau de exposição a riscos, trabalhando junto aos proprietários dos riscos e demais gestores na construção de matrizes de controles;
- Auxiliar no processo de avaliação dos riscos, especialmente no que tange a identificação dos controles internos existentes;
- Suportar os proprietários dos riscos na elaboração e implementação dos planos de ação para mitigação dos riscos;
- Auxiliar as demais áreas no (re)desenho de seus processos, de acordo com o plano de ação definidos em conjunto;
- Auxiliar os proprietários dos riscos no reporte do andamento da implementação dos planos de ação para a função de Gestão de Riscos;
- Estabelecer controles de forma a assegurar a efetividade da Matriz de Riscos.

5.6 Proprietários dos riscos

- Identificar, avaliar, tratar e monitorar os riscos relacionados, de forma a cumprir os objetivos estratégicos e em observância ao perfil de risco da PetroRio;
- Elaborar, sugerir e implementar os planos de ação e/ou de contingência para a mitigação dos riscos (com envolvimento de outras áreas, se necessário);
- Elaborar as fichas de riscos e atualizá-las periodicamente e sempre que necessário;
- Atuar no aprimoramento contínuo do ambiente de controles internos da PetroRio;
- Disseminar a cultura de gestão de riscos e controles internos para os demais integrantes de sua área;
- Comunicar tempestivamente a função de riscos ao identificar novos riscos ou alterações em riscos atuais;

- Implementar os planos de ação definidos em conjunto com as funções de Gestão de Riscos e Controles Internos a partir de cada risco identificado;
- Definir indicadores de risco (KRIs) para monitorar a variação e os resultados dos riscos corporativos sob sua responsabilidade;
- Efetuar reportes periódicos à função de riscos sobre o acompanhamento do risco sob sua responsabilidade;
- Efetuar reportes à Diretoria Executiva, Comitê de Ética e Compliance, e/ou Conselho de Administração quando demandado.

5.7 Função de Auditoria Interna

- Atuar no aprimoramento contínuo do ambiente de controles internos da PetroRio;
- Avaliar de forma independente e objetiva o processo de gestão de riscos da PetroRio;
- Avaliar de forma independente, objetiva e contínua os controles internos estabelecidos para os riscos priorizados e/ou com exposição superior ao apetite a risco da PetroRio;
- Estabelecer um plano de auditoria para avaliação dos processos internos da PetroRio conforme seu grau de exposição a risco;
- Avaliar a efetividade dos planos de ação implementados;
- Contribuir para o aprimoramento do ambiente de controles internos da PetroRio por meio de interações junto as áreas dos processos auditados, gerando recomendações e melhorias;
- Contribuir para melhorias no processo de tomada de decisão por meio de reporte dos resultados das auditorias independentes realizadas;
- Efetuar reportes à Diretoria Executiva, Comitê de Ética e Compliance e/ou Conselho de Administração acerca das avaliações realizadas.

6. Não Conformidade

6.1 Suspeita de Violação à Política e Medidas Disciplinares

Todos os incidentes ou suspeitas de violação desta Política serão tratados, dentro de limites razoáveis, de forma confidencial, a não ser quando a PetroRio esteja obrigada por força de lei ou ordem judicial a divulgar o incidente ou suspeita, e desde que a integridade física ou a vida de colaboradores da PetroRio e de quaisquer terceiros não esteja em risco, situação na qual a Companhia entende ser seu dever o imediato relato às autoridades competentes.

A não observância das diretrizes aqui expostas e das leis relacionadas a que a PetroRio está obrigada, inclusive por omissão, resultará na aplicação de medidas disciplinares e penalidades previstas em lei, além da responsabilização por perdas e danos causados à PetroRio e terceiros.

6.2 Reportando Preocupações no Canal de Integridade

Qualquer violação desta Política deverá ser reportada por meio do Canal de Integridade ou diretamente ao superior imediato e investigada pelo Comitê de Ética e Compliance, nos termos da Lei e da regulamentação aplicáveis. As informações registradas no Canal de Integridade ou reportadas diretamente ao superior imediato serão tratadas como confidenciais, sendo preservada a identidade do denunciante.

6.3 Não Retaliação

A todo momento serão preservados o sigilo, a identidade e a integridade daquele que, de boa-fé, informar fato ou suspeita de conduta violadora das normas desta Política.

* * *