POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

1. OBJETIVO

1.1. A presente Política de Gestão de Risco e Controles Internos da Ecorodovias Infraestrutura e Logística S.A. tem como propósito estabelecer as diretrizes, referências e responsabilidades relacionados às melhores práticas de governança corporativa no que diz respeito à gestão de riscos e controles internos do Grupo Ecorodovias.

1.2. A presente Política define as práticas aplicadas de maneira uniforme pelo Grupo Ecorodovias no que tange à identificação, avaliação, tratamento e monitoramento de riscos, de acordo com o seu objetivo estratégico.

1.3. A presente Política tem também o objetivo de formalizar e divulgar:

(i) O Programa de Gestão de Riscos e de Controles Internos do Grupo Ecorodovias; e
(ii) A cadeia de valor dos processos relacionados às práticas de Gestão de Riscos e de Controles Internos.

1.4. No Grupo Ecorodovias, a gestão de riscos e controles internos fornece à Alta Administração e aos demais gestores, instrumentos para a tomada de decisão, que permitem enfrentar as incertezas, visando reduzir a variabilidade futura dos resultados da empresa para alcançar benefícios.

2. APLICAÇÃO

2.1. Esta Política aplica-se ao Grupo Ecorodovias, à Alta Administração e aos Colaboradores, conforme aplicável.

3. REFERÊNCIAS

3.1. Utilizam-se como referência as melhores práticas de gestão de riscos e controles internos para empresas listadas no novo mercado, quais sejam:

(i) Norma ISO 37.001;
(ii) Norma ISO 31.000:2018;
(iii) Instrução CVM nº 480, de 7 de dezembro de 2009;
(iv) Regulamento de Listagem do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão, vigente a partir de 02 de janeiro de 2018;
(v) Código Brasileiro de Governança Corporativa – Companhias Abertas;
(vi) Código de Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC (“IBGC”);
(vii) Caderno de Governança Corporativa nº 19 do Instituto Brasileiro de Governança Corporativa (IBGC) Gerenciamento de Riscos; e

(viii) COSO (Commitee of Sponsoring Organizations of the Treadway) ERM (Enterprise Risk Management) 2017 Framework.

4. TERMOS E DEFINIÇÕES

- Alta Administração significa o Conselho de Administração, a Diretoria Estatutária e os Comitês de Assessoramento.

- Apetite a risco significa o nível de riscos que, de forma ampla, uma organização está preparada e disposta a assumir e gerenciar para atingir seus objetivos estratégicos na busca de valor, de acordo com os limites estabelecidos pela Alta Administração e aprovados pelo Conselho de Administração. O apetite a risco reflete na filosofia de gestão de riscos corporativos e, por sua vez, influencia a cultura e o estilo de operação.

- B3 significa a B3 S.A. – Brasil, Bolsa, Balcão.

- Colaborador(es) são todos os funcionários, incluindo os diretores não estatutários das empresas do Grupo Ecorodovias.

- Comitês ou Comitês de Assessoramento significam o Comitê de Gestão de Pessoas e Governança, o Comitê de Investimentos, Finanças e Risco, o Comitê de Auditoria, e os demais comitês de assessoramento criados ou instituídos pelo Conselho de Administração.

- Companhia ou Ecorodovias significa a Ecorodovias Infraestrutura e Logística S.A.

- Conselho de Administração significa o conselho de administração da Companhia.

- Controle Interno significa um processo da estrutura de governança conduzido para garantir o alcance dos objetivos organizacionais, em que eventos indesejáveis serão prevenidos, detectados e/ou corrigidos.

- CVM significa a Comissão de Valores Mobiliários.

- Diretor Presidente significa o diretor presidente da Companhia.

- Diretoria Estatutária significa a diretoria estatutária da Companhia.

- Dono do Risco (Risk Owner) são os gestores em nível executivo definidos pela IN de Organização e Regimento Interno responsáveis pelo tratamento dos riscos sob sua gestão.

- Dono do Controle (Control Owner) são os colaboradores responsáveis pela execução dos processos e controles, seguindo as diretrizes internas e garantindo a adequada mitigação dos

riscos. Devem comunicar ao gestor de mitigação dos riscos quando identificarem novos riscos ou oportunidades de melhorias nos processos.

- Gestor de Mitigação do risco (Risk Manager) significa os gestores responsáveis por garantir que os processos e os controles sob sua gestão serão executados conforme definido nas diretrizes internas, garantindo a adequada mitigação dos riscos.

- Grupo Ecorodovias significa a Companhia e suas sociedades controladas.

- KRI (Key Risk Indicators) significa os indicadores de riscos da Companhia que sinalizam as causas das mudanças no nível de risco dos negócios. Se percebidos em tempo hábil, ajudam a Companhia a agir preventivamente e reduzir perdas e/ou aproveitar novas oportunidades de criar, proteger e crescer seu valor.

- Política significa a presente Política de Gestão de Riscos e Controles Internos.

- Programa de Gestão de Riscos e de Controles Internos ou Programa de Gestão de Riscos significa o programa descrito no item 5.1 desta Política.

- Regulamento do Novo Mercado significa o Regulamento para Listagem de Emissores e Admissão à Negociação de Valores Mobiliários da B3.

- Risco significa a possibilidade de desvios adversos em relação aos valores esperados no futuro. No processo de avaliação dos riscos, analisamos o Risco Inerente, que se constitui na análise do Risco sem considerar os efeitos dos controles e o Risco Residual, que é a avaliação do Risco considerando o efeito dos controles internos existentes.

No Grupo Ecorodovias, o Programa de Gestão de Riscos e de Controles Internos fornece à Alta Administração e aos demais gestores instrumentos para tomada de decisão, que permitem enfrentar as incertezas, visando reduzir a variabilidade futura dos resultados da empresa para alcançar benefícios como:

(i) Menor possibilidade de perdas inesperadas e maior probabilidade de alcance de objetivos e metas;
(ii) Base alargada de informações para a tomada de decisões;
(iii) Otimização da alocação de capital, com geração sistemática de valor para os acionistas;
(iv) Confiança para alavancar a empresa financeira e operacionalmente, bem como entrar em novos negócios;
(v) Redução nas chances de não cumprimento de exigências legais e regulatórias;
(vi) Demonstrações financeiras mais confiáveis e maior transparência para as partes interessadas;
(vii) Melhora dos processos internos com eliminação de controles redundantes e/ou não efetivos;
(viii) Maior efetividade operacional e eficiência de custos.

5. PROGRAMA DE GESTÃO DE RISCOS E CONTROLES INTERNOS DO GRUPO ECORODOVIAS

O programa de Gestão de Riscos e Controles Internos foi definido com base nas práticas recomendadas pelo COSO ERM e pela norma ISO 31000:2018 e trata da implementação por meio da aplicação dos princípios e diretrizes gerais estipulados pela Diretoria Estatutária por meio do "Plano Diretor de Gestão de Riscos e Controles Internos" do Grupo, definindo a forma como os riscos devem ser identificados, mensurados e geridos e, ainda, como os controles internos devem ser periodicamente avaliados, testados e comunicados.

O Programa de Gestão de Riscos permeia toda a cadeia de valor do Grupo Ecorodovias, ou seja, todo o conjunto de atividades que o Grupo, como organização, realiza para criar valor a todas as partes interessadas, visando o cenário de segurança, sustentabilidade e amadurecimento constante dos procedimentos internos que suportam os negócios da companhia, podendo ser refletido no processo representado na Figura 1 abaixo.

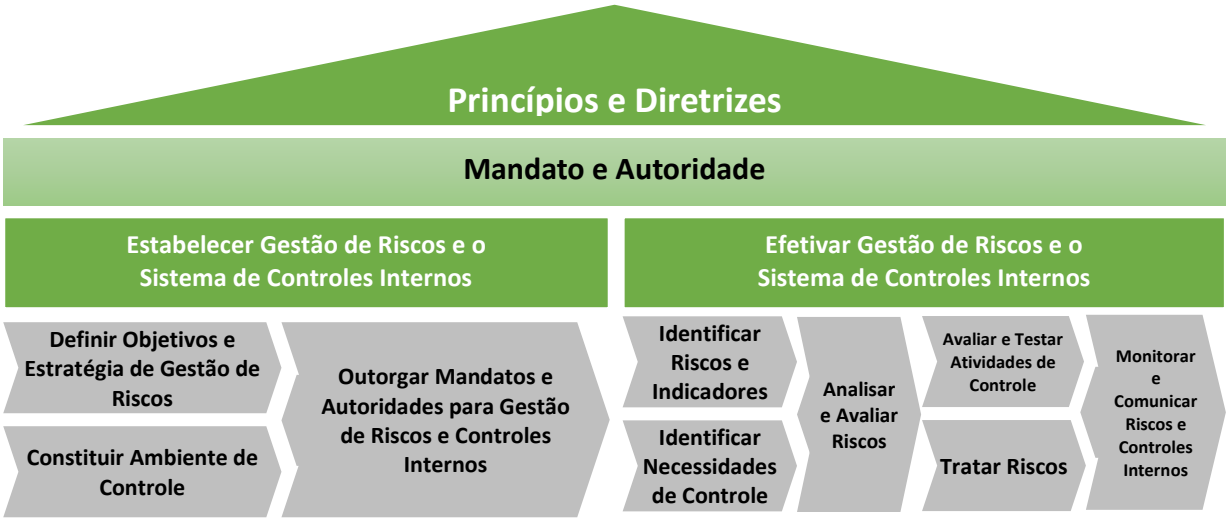

Figura 1 – Programa de Gestão de Riscos e de Controles Internos do Grupo Ecorodovias.

5.1 Estabelecer a Gestão de Riscos e o Sistema de Controles Internos

Os componentes desta parte do processo constituem a estrutura que irá sustentar todo o gerenciamento de riscos. Compreendem avaliações relativas a:

- Contexto: organização, expectativas dos stakeholders e escopo do sistema de gestão;
- Liderança: comprometimento, políticas e papéis-responsabilidades organizacionais; e
- Apoio: recursos, competências, consciência, comunicação e documentação.

5.1.1 Definir objetivos e Estratégia da Gestão de Riscos

Gerenciamento de riscos corporativos é o processo de planejar, organizar, liderar e controlar as atividades de uma organização a fim de minimizar os efeitos do risco na sua posição financeira.

Deve estar intrínseco às atividades e funções da organização, e o modo como ela funciona deve ser personalizado para os interesses da organização de acordo com o planejamento e os objetivos estratégicos.

A estratégia de gestão dos riscos do Grupo Ecorodovias apoia-se e organiza-se em dois pilares complementares:

Gestão Macro ou Holística

A gestão no Nível Macro tem caráter eminentemente estratégico, pois está intrinsicamente ligada a questões como missão, visão e objetivos empresariais, ambiente regulatório e competitivo, e capacidade financeira, visando também a compreensão integral dos riscos: considera o potencial impacto de todos os tipos de riscos sobre todos os processos, atividades, *stakeholders*, produtos e serviços. É nesse nível que são definidos dois importantes direcionadores (drivers) da própria estratégia empresarial do Grupo Ecorodovias:

- **Apetite a risco:** (i) representa a gama de riscos que a organização, na sua busca de valor, decide aceitar para realizar a própria missão/visão; (ii) é um conceito relacionado a desejo; e (iii) deve ser consistente com os objetivos estratégicos, o ambiente regulatório, as condições de competitividade e a capacidade da empresa de gerenciar riscos de forma efetiva e prudente;
- **Tolerância a risco:** (i) diz respeito ao nível de desvio em relação às metas e objetivos definidos na estratégia que seja compatível com a capacidade de absorção da empresa; e (ii) é um conceito relacionado a capacidade, ou limite.

O Apetite a risco mudará de acordo com os cenários que a Companhia encontrará e objetivos estratégicos definidos pela Administração e aprovados pelo Conselho de Administração.

Esse pilar da gestão dos riscos corporativos é por definição construído e operacionalizado de maneira centralizada, pois emprega recursos e informações disponíveis a Diretoria Estatutária da Companhia que também exerce papel de supervisão sobre todas as atividades do Programa de Gestão de Riscos e Controles Internos do Grupo.

A abordagem é dita top-down porque:

(i) as ações da gestão micro podem ser orientadas para focar nos fatores que mais contribuem para o risco agregado (macro); e
(ii) a alocação de recursos para as unidades operacionais é função da contribuição de cada unidade para a matriz risco-retorno do Grupo.

Gestão Micro ou Individualizada

A gestão micro ou individualizada de cada risco contempla o conjunto de ações gerenciais voltadas à identificação, análise, avaliação, tratamento e monitoramento de um determinado tipo de risco.

O Gerenciamento Micro realizado nas unidades de negócio e nas áreas funcionais corporativas é hierarquicamente subordinado e alinhado ao Gerenciamento Macro conduzido pela Diretoria Estatutária da Companhia. Sob a perspectiva da gestão micro de riscos, todos os colaboradores da Companhia são considerados Gestores de Riscos, ou seja, agentes com potencial para identificar riscos em suas atividades, analisá-los (objetiva ou subjetivamente), tratá-los e monitorá-los.

A implementação da metodologia padrão para gestão de riscos exige que todos os processos sejam avaliados. A operacionalização, descentralizada pela própria natureza, é desenvolvida nas unidades operacionais e intensiva em recursos humanos e tecnológicos.

Consequentemente, essa metodologia *bottom-up* produz um enorme catálogo de riscos que precisa ser agrupado para que seja viável a priorização das ações na organização como um todo e a definição de uma estratégia de mitigação otimizada, podendo ser refletido no processo representado na Figura 2 abaixo.

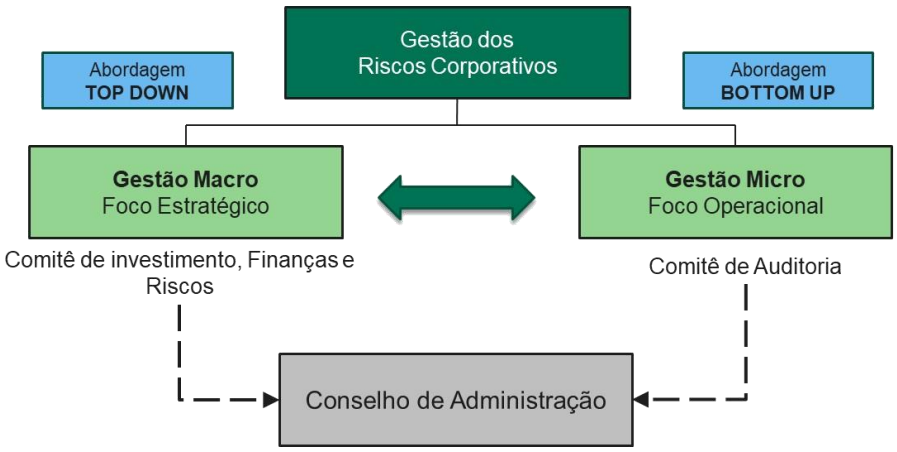

Figura 2 – Organização da gestão de risco

5.1.2 Construir Ambiente de Controle

O ambiente de controle envolve um conjunto de normas, processos e estruturas que fornece a base para que a organização mantenha efetividade e eficiência em seus processos, possua confiança nos relatórios e informações financeiras e esteja em conformidade com as leis e regulamentos aplicáveis. É composto por estruturas, normas, processos e outros mecanismos adotados para mitigar riscos.

Podem ser definidos como:

- Controles a nível de entidade - “Entity Level Controls”: possuem efeito propagador nas atividades de controle de toda a estrutura organizacional.
- Controles de nível de processo: são atividades executadas que visam mitigar riscos, tais como revisão, aprovações etc.

5.1.3 Responsabilidades e Atribuições

A outorga de mandatos e autoridades diz respeito tanto às políticas e procedimentos definidos e formalizados pela Companhia quanto à definição dos papéis e responsabilidades distribuídos para implementação das práticas de Gestão de Riscos e Controles Internos em toda a Organização.

O Conselho de Administração é o responsável primário pela definição deste Programa que estabelece que mandatos e autoridades sejam adequadamente atribuídos para que, em última instância, a responsabilidade seja delegada a executivos, gestores e colaboradores em todos os níveis e Unidades de negócio da organização.

A estrutura organizacional que sustenta a gestão de riscos e o sistema de controles internos, incluindo-se uma breve descrição dos papéis e responsabilidades dos principais agentes, é apresentada neste documento. A supervisão é compartilhada pelos órgãos que compõem a Diretoria Estatutária do Grupo Ecorodovias, enquanto os agentes de execução que compõem as ‘Três Linhas de Defesa’ são responsáveis pela efetivação da gestão de riscos e pela operacionalização do sistema de controles internos, conforme se verifica na imagem 3, abaixo.

Figura 3 – Organograma de linhas de defesa na gestão de riscos e controles internos, figura adaptada do modelo do IIA.

Conselho de Administração

Compete ao Conselho de Administração no âmbito desta Política, sem prejuízo das demais competências definidas em seu regimento interno:

- Com o apoio dos Comitês de Assessoramento, aprovar a política de Gestão de Riscos e Controles Internos compatíveis com as estratégias de negócios do grupo;

- Avaliar e monitorar periodicamente a exposição da companhia a riscos e a eficácia dos sistemas de Gestão de Riscos e Controles, verificando se estão compatíveis com as estratégias de negócios;
- Aprovar o nível de Apetite e Tolerância a Risco da Companhia na condução de seus negócios;
- Acompanhar o cumprimento dos parâmetros de riscos definidos nesta Política de Gestão de Riscos e Controle Interno;
- Conscientizar os gestores sobre a importância da Gestão de Riscos e Controle Interno e a responsabilidade inerente aos Administradores e Colaboradores da Companhia.

Comitê de Auditoria

Compete ao Comitê de Auditoria, no âmbito desta Política, sem prejuízo das demais competências definidas em seu regimento interno:

- Analisar a Política de Gestão de Riscos da Companhia, assim como quaisquer revisões, submetendo-a à aprovação do Conselho de Administração;
- Acompanhar de forma sistemática a gestão de riscos e o cumprimento de seus objetivos;
- Supervisionar as atividades da área de controles internos da Companhia e de suas controladas;
- Avaliar a efetividade e a suficiência dos sistemas de controles e de gerenciamento de riscos operacionais;
- Assegurar que estejam definidos os responsáveis pelo monitoramento de cada risco e as segregações de funções sejam respeitadas;
- Avaliar se a divulgação dos itens “Fatores de risco” e “Risco de Mercado” no Formulário de Referência da CVM refletem a visão da gestão de riscos da companhia, assim como se a divulgação está coerente com as notas explicativas.

Diretoria Estatutária

Compete à Diretoria Estatutária no âmbito desta Política, sem prejuízo das suas demais competências:

- Revisar e executar a Política de Gestão de Riscos e Controle Interno e, sempre que necessário, propor a revisão dessa política, em função de alterações nos riscos a que a companhia está exposta;
- Implementar e manter mecanismos, processos e programas eficazes de monitoramento e divulgação do desempenho financeiro e operacional e dos impactos das atividades da companhia na sociedade e no meio ambiente;
- Avaliar, pelo menos anualmente, a eficácia das políticas e dos sistemas de Gestão de Riscos e Controles Internos e prestar contas ao Conselho de Administração sobre essa avaliação;
- Todo (a) diretor (a) responde ao nível hierárquico imediatamente superior por sua parcela de gestão de riscos, cabendo ao Diretor (a) Presidente responsabilidade final perante o Conselho de Administração;
- Atuar na atualização do mapa de riscos dentro da sua área de competência;
- Definir as diretrizes e assegurar recursos que garantam o bom funcionamento e a eficácia do Gestão de riscos e Controle Interno;

- Promover a integração das atividades de Gestão de Riscos e Controle Interno com os ciclos de planejamento e gestão do Grupo Ecorodovias; e
- Interagir com os Comitês do Conselho em questões relativas a Gerenciamento de Riscos.

Diretor Presidente

Compete ao Diretor Presidente, no âmbito desta Política:

- Atuar como responsável final pela Gestão de Riscos e Controle Interno do Grupo Ecorodovias;
- Definir as diretrizes e assegurar recursos que garantam o bom funcionamento e a eficácia da Gestão de Riscos e Controle Interno; e
- Promover a integração das atividades de Gestão de Riscos e Controle Interno com os ciclos de planejamento e gestão do Grupo Ecorodovias.

Comitê de Investimentos, Finanças e Risco

Compete ao Comitê de Investimentos, Finanças e Risco no âmbito desta Política:

- Acompanhar e informar o Conselho de Administração sobre questões financeiras-chave relacionadas à análise de risco financeiro e de mercado, tais como:
- Exposições ao câmbio;
- Aval em operações;
- Nível de alavancagem, financiamentos e garantias;
- Política de dividendos;
- Emissão de ações e de títulos da dívida e investimentos;
- Novos negócios, fusões e aquisições;
- Orçamento anual; e
- Destinação de resultados e distribuição de dividendos.

Gerência de Riscos e Controles Internos

Compete à Gerência de Riscos e Controles Internos, no âmbito desta Política:

- Atuar como responsável pela Gestão de Riscos e Controle Internos, incluindo sua avaliação, consolidação, e priorização dos riscos;
- Propor ao Conselho de Administração, com apreciação prévia da Diretoria Estatutária, do Comitê de Auditoria ou de Riscos e Investimentos, as edições desta Política e o nível de Apetite à Risco do Grupo Ecorodovias;
- Exercer papel consultivo junto aos donos dos riscos, gestores dos riscos e donos dos controles, apoiando-os na identificação e tratamento;
- Desenvolver e disponibilizar as metodologias, ferramentas, sistemas, infraestrutura e governança necessárias para suportar a Gestão de Riscos e Controles Internos;
- Monitorar e avaliar os eventos de risco relevantes e os respectivos desvios em relação ao apetite a risco estabelecido e aprovado;
- Coordenar a integração das atividades relativas a Gerenciamento de Riscos do Comitê de Auditoria (Nível Micro) e do Comitê de Investimentos, Finanças e Riscos (Nível Macro);

- Desenvolver programas de comunicação interna (endomarketing) relativos às atividades de Gestão de Riscos e Controles Internos, disseminando conceitos, metodologias e o uso de ferramentas, informando o estágio de desenvolvimento das iniciativas e os resultados esperados e divulgando as informações julgadas importantes sobre estes temas;
- Propor cronograma operacional anual para a realização das atividades de Gestão de Riscos e de Controles Internos no Grupo;
- Apurar o resultado dos indicadores de performance, acompanhar a evolução e tendências no mercado (melhores práticas) e elaborar sugestões de melhoria contínua para ajustes na Gestão de Riscos e nos Controles Internos;
- Reportar os riscos críticos e respectivas exposições para o Conselho de Administração, com apreciação prévia do Comitê de Auditoria (Nível Micro) e do Comitê de Investimentos, Finanças e Riscos;
- Patrocinar a implantação da Gestão de Riscos e Controles Internos na Companhia; e
- Acompanhar a implantação e Follow up das recomendações para a melhoria e/ou correções do ambiente de controles, e a apresentação dos resultados destas implementações para a Diretoria Estatutária e Comitê de Auditoria, conforme calendário de pautas pré-estabelecidos ou quando demandado. Deverá assegurar que as recomendações sejam efetivamente implementadas ou que a Diretoria tenha aceitado o risco de não efetuar a respectiva implementação.

Diretoria de Compliance e Governança

Compete à Diretoria de Compliance e Governança, no âmbito desta Política:

- Realizar, com o auxílio da Gerência de Riscos e Controles Internos, a análise periódica de riscos de corrupção e suborno os quais o Grupo Ecorodovias está exposto, em especial quanto à efetividade e suficiência da estrutura de controles internos e dos processos;
- Elaborar e apresentar à alta administração relatório com plano de ação visando mitigar os riscos e fragilidades durante a auditoria interna e o monitoramento contínuo do PE – SI (Programa de Ética - Sistema de Integridade);
- Executar e apresentar à alta administração análises críticas periódicas para avaliar a eficácia do PE – SI; e
- Implementar as medidas destinadas à correção das deficiências identificadas e melhorias do ambiente de controles no âmbito do monitoramento do PE – SI.

Gerência de Auditoria Interna

Compete à Gerência de Auditoria Interna, no âmbito desta Política:

- Avaliação independente (Assurance) sobre a eficácia dos processos, controles internos e demais elementos de governança corporativa (Riscos, Compliance, etc);
- Auxiliar na verificação e cumprimento dos deveres legais e estatutários;
- Reporte dos resultados e das fragilidades identificadas a Alta Administração e a Comitê de Auditoria;
- Elaboração e executar o plano de auditoria aprovado pelo Comitê de Auditoria, com base em riscos, transações e processos críticos, sugestões dos executivos e histórico;
- Atuar com independência e imparcialidade; e

- Auxiliar as áreas operacionais a compreender os controles, as normas e as políticas estabelecidas.

Colaboradores

Compete aos Colaboradores no âmbito desta Política:

- Conscientizar-se dos Riscos inerentes às suas respectivas áreas de responsabilidade e de seu papel na gestão de Riscos de sua área;
- Participar de treinamentos sobre o tema Gerenciamento de Riscos;
- Reportar imediatamente a identificação de qualquer fato relevante, deficiência, falha ou não conformidade referente aos Riscos da Companhia aos Gestores dos Riscos; e
- Identificar e reportar aos Gestores dos Riscos eventuais Riscos ainda não mapeados.

5.2 Efetivar Gestão de Riscos e o Sistema de Controles Internos

Esta parte do sistema de gestão engloba os componentes que representam o próprio processo de gerenciamento de riscos, compreendendo:

- Planejar: objetivos do sistema de gestão e planejamento para alcançá-los;
- Implementar: planejamento operacional, implementação e controle;
- Mensurar: monitoramento, quantificação, análise, avaliação, auditoria e revisão; e
- Aprender: não-conformidade, ação corretiva e melhoria contínua.

A partir das premissas do programa de gestão de riscos e de controles internos, as seguintes etapas são executadas, conforme representado na Figura 4:

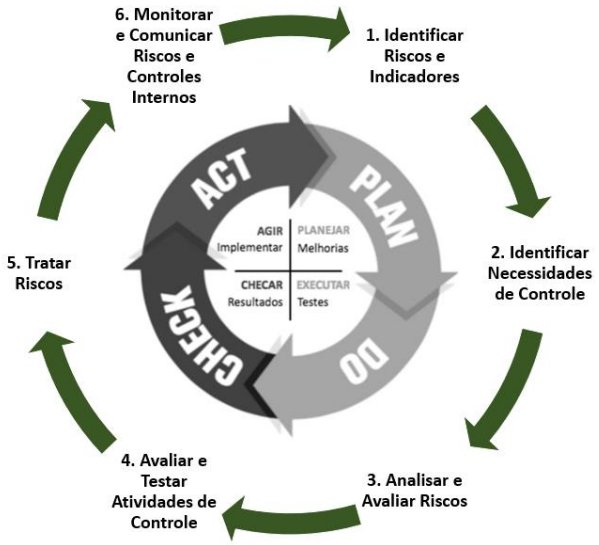

Figura 4 – Etapas da gestão de riscos e controles internos

5.2.1 Identificar Riscos e Indicadores

No Grupo Ecorodovias, a identificação de riscos é realizada de forma corporativa por meio das abordagens *top-down* e *bottom-up*.

Na abordagem *top-down* (gestão no nível macro) são identificados os riscos corporativos com potencial para impactar significativamente o cumprimento dos objetivos estratégicos da companhia. Envolve a análise do ambiente externo - ameaças e oportunidades.

Os riscos identificados, predominantemente de natureza estratégica, são sintetizados no (restrito) Inventário de Riscos Estratégicos. A reavaliação periódica desse elenco de riscos está incorporada no processo de elaboração e acompanhamento da execução do Planejamento Estratégico e de reuniões periódicas com a Diretoria Estatutária da Companhia para atualização do Mapa de Riscos do Grupo.

Na abordagem *bottom-up* (gestão no nível micro) são identificados os riscos relativos a processos da cadeia de valor da Companhia (gestão, negócio e apoio) que podem impactar a realização das funções desses processos. Suas atividades estão relacionadas à identificação dos riscos operacionais, financeiros e de conformidade (*compliance*), abrangendo, portanto, dezenas de tipos de risco. A revisão periódica é atrelada às atividades rotineiras de gestão de riscos, controles internos e auditoria, sujeitas a acompanhamento e monitoramento recorrentes.

A classificação dos riscos estratégicos da companhia está disposta em 4 categorias, e são compostos por tópicos denominados “fatores de risco”:

Categoria	Descrição
Riscos estratégicos	Riscos assumidos na busca de retornos estratégicos superiores e relacionados às oportunidades. Decorre de movimentos adversos às estratégias selecionadas pela Corporação, sejam eles endógenos ou exógenos.
Riscos financeiros	É o risco de que os fluxos de caixa não sejam administrados efetivamente para maximizar a geração de caixa operacional, gerenciar os riscos e retornos específicos das transações financeiras e captar e aplicar recursos financeiros de acordo com as políticas estabelecidas.
Riscos operacionais	Decorrente da falta de consistência e adequação dos sistemas de informação, processamento e controle de operações, bem como de falhas nos controles internos ou fraudes que prejudiquem o exercício das atividades da Companhia.
Riscos de *compliance*	São os riscos relacionados com a falta de habilidade ou disciplina para cumprir com a legislação e/ou regulamentação aplicáveis ao negócio e as normas e procedimentos internos.

5.2.2 Identificar necessidades de controles

Atividades de controle são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela Diretoria Estatutária para mitigar riscos que poderiam dificultar a realização dos objetivos. São desempenhadas em todos os ambientes e níveis da organização, incluindo os processos corporativos e o ambiente tecnológico e de infraestrutura. Podem ser de natureza preventiva-identificativa e incorporar atividades manuais e/ou automáticas.

No Grupo Ecorodovias, as necessidades de controle são permanentemente identificadas e soluções são desenvolvidas, monitoradas e aperfeiçoadas a fim de mitigar os riscos identificados e acentuar a efetividade e a eficiência das atividades de controles.

Para o Grupo Ecorodovias, as atividades de controle são classificadas considerando seus atributos, como:

- Frequência: quantidade de ocorrências dentro do período avaliado;
- Tipo do Controle: que pode ser diretivo, preventivo ou detectivo;
- Nível de automatização: que pode ser automático, manual ou dependente de TI;
- Maturidade do controle: que pode ser informal, padronizado, automatizado ou monitorado.

5.2.3 Analisar e Avaliar Riscos

A análise e avaliação de riscos tem por propósito a compreensão da natureza do risco e suas características. Envolve a consideração detalhada de incertezas, fontes e fatores de risco, probabilidade de eventos, natureza e magnitude das consequências, cenários e eficácia dos controles existentes. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos, e a consequência de um risco pode ser a causa de outro. As técnicas de análise podem ser qualitativas, quantitativas ou uma combinação destas, dependendo das informações e recursos disponíveis.

Cada risco deve ser analisado individualmente quanto à probabilidade de ocorrência e impacto, e deve ser alocado na matriz de risco construída pela companhia. Com isso, a companhia poderá implementar, de forma efetiva, o Programa de Gestão de Riscos e de Controles Internos. Essa abordagem não difere entre *top-down* e *bottom-up*.

O propósito da avaliação de riscos é apoiar decisões. Envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de: (i) aceitar o risco; (ii) considerar as opções de tratamento de riscos; (iii) transferir o risco; (iv) manter os controles existentes; e (v) reconsiderar os objetivos.

O fluxo realizado pela Companhia para a avaliação dos riscos está representado na Figura 5:

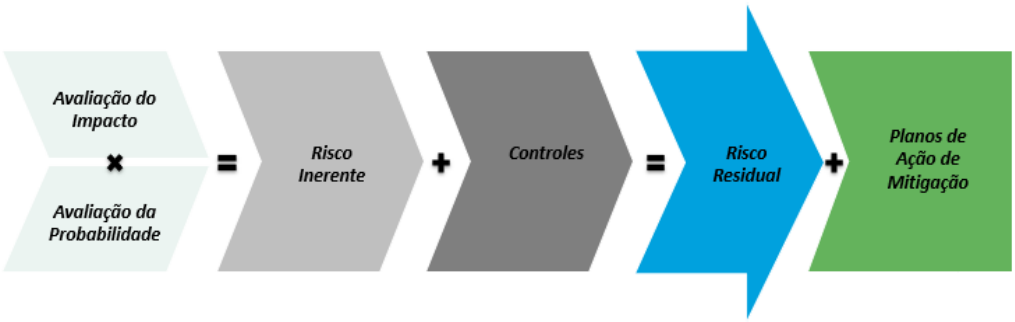

Figura 5 – Fluxo de análise de riscos

Adicionalmente, no Nível Macro de gestão emprega-se Análise de Cenários, no qual para definir limites plausíveis para os futuros estados da variável de interesse. O grupo de análise (experts) seleciona e examina os direcionadores (drivers) que causariam o maior impacto na companhia, e os consideram na elaboração de cenários julgamentais (isto é, fundamentados em critérios subjetivos). O efeito agregado de todos os demais fatores é estimado como uma fração do efeito dos fatores principais.

5.2.3.1 Definição de escala de Impacto x probabilidade

Para a avaliação dos riscos o Grupo Ecorodovias utiliza da métrica "impacto x probabilidade", onde:

Impacto: Considera-se uma avaliação quantitativa e qualitativa do risco nos quesitos de conformidade legal, reputacional, socioambiental e impacto econômico, sendo as métricas financeiras baseadas em percentuais do "EBITDA".

Escala de impacto: Crítico, Alto, Médio e Baixo

Probabilidade: Define-se como a probabilidade de materialização do evento de risco durante um determinado período, considerando o histórico de ocorrências ou previsões futuras.

Escala de Probabilidade: Muito provável, Provável, Pouco Provável e Improvável

5.2.3.2 Análise de risco inerente e residual

Desta forma, a companhia utiliza 2 cenários para avaliação dos riscos, sendo:

Risco Inerente: É o resultado da avaliação dos riscos (impacto x probabilidade) considerando um cenário em que não há nenhuma ação da companhia para mitigá-lo, ou seja, em seu estado potencial, ausente de controles.

Risco Residual: É o resultado da avaliação dos riscos (impacto x probabilidade) considerando os controles existentes e seu potencial de mitigação destes riscos. A atuação dos controles, se efetiva, tende a reduzir o impacto dos riscos e ou a probabilidade de ocorrência.

5.2.3.3 Severidade dos Riscos

A severidade do risco é definida a partir do cruzamento das notas atribuídas de impacto e probabilidade, sendo classificada conforme escala abaixo:
Escala de severidade: Crítico, Alto, Médio e Baixo

Riscos classificados no quadrante crítico da matriz deverão possuir planos de ação para tratamento, visando redução de severidade (respeitando as definições do item "2.2.4 Tratar Riscos"). Caso se opte por decisões que não envolvam a mitigação do risco, este deve ser submetido ao acompanhamento do Conselho de Administração.

5.2.3.4 Avaliar e testar atividades de controle

A avaliação e o teste das atividades de controle têm por objetivo verificar a efetividade do desenho e da operação para a qual o controle foi estabelecido. No Grupo Ecorodovias essa avaliação é realizada de maneira sistemática por meio de *walkthroughs* (literalmente 'percorrer o processo') e de métodos de indagação, observação, exame e re-execução a serem aplicados conforme a disponibilidade de dados e à criticidade da exposição aos riscos associados.

Os responsáveis pela realização dos testes de verificação dos controles são os agentes de execução da gestão de riscos e operacionalização do sistema de controles internos que compõem as chamadas 2ª. Linha de defesa (Gerência de Riscos e Controles Internos e Diretoria de Compliance e Governança) e 3ª. Linha de defesa (Auditoria Interna do Grupo).

5.2.4 Tratar Riscos

Uma vez efetivados os processos de identificação, análise e avaliação dos riscos e controles, deve-se definir e implementar uma estratégia para tratamento dos riscos. O propósito do tratamento é selecionar opções para abordar riscos, e envolve um processo interativo de:

(i) formular e selecionar opções;
(ii) planejar e implementar;
(iii) avaliar a eficácia.
(iv) decidir se o risco remanescente é aceitável; e
(v) se não for aceitável, realizar tratamento adicional.

A seleção da(s) opção(ões) mais apropriada(s) envolve harmonização do dilema, benefícios potenciais *versus* custos, esforços e desvantagens da implementação, tanto na gestão Micro quanto na Macro. As opções podem envolver um ou mais dos seguintes:

(i) evitar o risco;
(ii) assumir ou aumentar o risco;
(iii) remover a fonte de risco;
(iv) mudar a probabilidade;
(v) mudar as consequências;
(vi) compartilhar o risco; e
(vii) reter o risco.

5.2.4.1 Planos de Ação de Riscos e Controles Internos

A partir das avaliações periódicas dos riscos e avaliações dos ambientes de controles, bem como as ações geradas nas auditorias internas e externas, independente da origem da avaliação, surge a necessidade de se elaborar e executar o "plano de ação", visando a melhoria contínua do ambiente de controles internos e redução dos riscos do Grupo. As ações são definidas pelos gestores de mitigação dos riscos com o suporte técnico da Gerência de Riscos e Controles Internos e devem possuir as datas que efetivamente devem ser concluídos.

Nas análises dos planos de ação, podem ocorrer de alguns riscos estarem dentro do apetite da companhia, ou seja, eles são aceitos e não são determinadas ações de mitigação. Essa deliberação é realizada pelo Comitê de Auditoria.

O monitoramento dos planos de ação é realizado pela área de Riscos e Controles Internos e periodicamente, executados follow-up das ações com as áreas de negócio. Nos casos em que as ações não são concluídas nos prazos acordados e as áreas de negócio necessitam de reprogramações, os prazos são realinhados considerando o seguinte critério:

a) **Riscos com rating baixo e médio:** a reprogramação deve ser aprovada pelo Risk Owner;
b) **Riscos com rating Alto:** a reprogramação, além de ser aprovada pelo Risk Owner, deve ser submetida ao Comitê de Auditoria para aprovação.

Os reportes dos follow-ups devem ser realizados no mínimo, 2 vezes ao ano ao Comitê de Auditoria e as recomendações para possíveis ajustes ou melhorias, são direcionadas pela área de Riscos e Controles Internos.

5.2.5 Monitorar e Comunicar Riscos e Controles Internos

Monitoramento e análise crítica visam assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados dos processos, e ocorrem em todos os seus estágios. Informações detalhadas sobre riscos e controles internos auxiliam os administradores da Companhia a compreender e tomar decisões relativas aos riscos avaliados e à efetividade dos controles. Consequentemente, é vital que essas informações cheguem tempestivamente aos agentes interessados.

No Grupo Ecorodovias, esses relatórios são compartilhados com membros dos comitês estatutários e não estatutários e circulados nos diversos fóruns internos de discussão. Informações sobre fatores de riscos e mecanismos de mitigação e fatos relevantes são publicados periodicamente ou sob demanda de *stakeholders* (poderes concedentes, acionistas, credores, usuários, clientes, comunidades, etc.) e de reguladores (Comissão de Valores Mobiliários, Anbima, B3, ANTT, Codesp e outros).

5.2.5.1 Atualização do mapa de riscos:

A atualização do mapa de riscos deve ocorrer no mínimo duas vezes ao ano ou:

- Quando houver mudanças significativas na estrutura interna e/ou nos ambientes de negócio com impacto nas operações da empresa e/ou nos processos;
- Quando houver mudanças regulatórias ou de legislações, que possam ter impacto na análise dos riscos;
- Quando houver demandas específicas do conselho de administração para tomada de decisão estratégica;
- Quando houver a necessidade específica atrelada ao planejamento estratégico da companhia, entre outras.

5.2.5.2 Frequência de reporte:

O reporte do mapa de risco deve ocorrer no mínimo duas vezes ao ano para a administração da companhia e anualmente para o Comitê de Auditoria e Conselho de Administração, ou conforme necessidade.

6. ASPECTOS GERAIS

6.1. A Diretoria de Planejamento, Estratégia Financeira e Riscos será responsável por promover treinamentos periódicos para o engajamento e conscientização das pessoas sujeitas a esta Política, no intuito de orientar ao cumprimento das diretrizes aqui previstas.

6.2. Dúvidas acerca das considerações dispostas neste documento podem ser esclarecidas pela Gerência de Riscos e Controles Internos do Grupo Ecorodovias.

7. APROVAÇÃO E VIGÊNCIA

7.1. Esta Política foi revisada e aprovada pelo Conselho de Administração em reunião realizada em 24 de março de 2022 e entra em vigor a partir desta data.