

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

1. OBJETIVO

Fornecer as diretrizes gerais para a gestão de risco, visando conceituar e documentar os princípios de Gestão de Riscos e atividades relacionadas.

2. ABRANGÊNCIA

Aplica-se à Eletropaulo Metropolitana Eletricidade de São Paulo S.A. (“Eletropaulo” ou “Companhia”). Áreas que apresentam processos de Gestão de Riscos devem estar em linha com a Política de Gestão de Riscos vigente.

3. DIRETRIZES

As diretrizes apresentadas nessa política definem os macroprocessos de Gestão de Riscos e a governança aplicada para o seu devido funcionamento.

3.1 Identificações de Riscos e Eventos

A identificação de riscos e eventos na Eletropaulo, ocorre de maneira estruturada em linha com as estratégias de negócio da Companhia, por meio de:

- Fontes internas:
 - Anualmente os principais executivos são entrevistados para identificação de tendências e novos riscos;
 - Responsável pelo risco, demais colaboradores e auditores internos.
- Fontes externas:
 - Auditores externos, órgãos reguladores, mercado, governo, mídia e demais partes interessadas.

Suas descrições obedecem a um formato estruturado para facilitar sua identificação, avaliação e monitoramento.

Os riscos são classificados pelas tipologias de riscos e seguirão para avaliação de riscos e tratamento.

3.2 Avaliação de Riscos e Tratamento

O responsável pelo risco, juntamente com a área de Gestão de Riscos, deve avaliar os riscos pelo seu impacto e probabilidade de ocorrência e utilizar metodologias de mensuração quantitativa e/ou qualitativa.

Essa avaliação leva em consideração a combinação entre probabilidade e impacto:

- Impacto quantitativo: medido pelo impacto potencial em valores financeiros;
- Impacto qualitativo: por exemplo, Reputação e Imagem.

A definição do tratamento a ser dado aos riscos identificados baseia-se no seu grau de exposição e natureza de risco. O grau de exposição é classificado como “Muito Baixo”, “Baixo”, “Médio”, “Alto” ou “Muito Alto” tanto para impacto quanto para probabilidade.

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

Quando for possível uma abordagem quantitativa, a Eletropaulo utiliza a materialidade de exposição ao risco em determinado percentual de um indicador financeiro (como EBITDA ou Lucro Líquido) acumulado em 31 de dezembro do exercício anterior ao ano corrente.

A escala de materialidade tanto para o impacto quanto para a probabilidade de ocorrência de um risco mapeado é considerada:

- (i) “muito baixa” quando o impacto representa <20%;
- (ii) “baixa” quando impacto representa entre 20,01% até 40%;
- (iii) “média” quando impacto representa entre 40,01% até 60%;
- (iv) “alta” quando impacto representa entre 60,01% até 80%;
- (iv) “muito alta” quando impacto representa >80%.

Após a avaliação do risco, o tratamento envolve a seleção de uma ou mais opções para tratar os riscos e a posterior implementação de controles e/ou processos para acompanhamento do próprio.

As alternativas de tratamento dos riscos são:

- Eliminar o risco
- Diminuir o risco
- Transferir o risco
- Aceitar o risco

Na hipótese de a Companhia utilizar de instrumentos financeiros derivativos para tratar os riscos, esse uso fica restrito para fins exclusivos de proteção (*hedge*). Esse processo é regido por procedimento interno específico que atende às diretrizes do Estatuto Social da Companhia.

3.3 Apetite a Riscos e delimitação de Limites de Riscos Aceitáveis

O apetite e os limites à risco da Companhia, são definidos pelo Conselho de Administração e devem estar alinhados com as respectivas estratégias da empresa e estar refletido nos limites de riscos aceitáveis pela Companhia.

Estes limites são propostos pelo Comitê Executivo de Gestão de Riscos e discutidos junto ao Comitê de Auditoria e submetidos ao Conselho de Administração, e estão associados ao grau de exposição de riscos que a Companhia está disposta a aceitar para atingir seus objetivos estratégicos e criar valor para os acionistas.

3.4 Monitoramento

A área de Gestão de Riscos deve acompanhar o desempenho dos indicadores de riscos bem como os seus limites e supervisionar a implementação e manutenção dos planos de ação através de gestão contínua e avaliações independentes.

As atividades de Gestão de Riscos devem ser adequadamente documentadas como forma de evidenciar sua aderência ao modelo de Gestão de Riscos da Companhia.

3.5 Comunicação e consulta

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

O processo de comunicação e consulta de riscos é parte integrante do processo de Gestão de Riscos, e é parte integrante da cultura de riscos. Uma vez identificados, avaliados e monitorados, fazem parte do processo de comunicação interna, que permeiam a Companhia e que visam compartilhar e fornecer informações para o gerenciamento contínuo de riscos.

3.6 Priorização de riscos e mapa de riscos (“*heat map*”)

Após a análise de riscos, é feita a comparação quanto aos níveis de impacto e probabilidade atribuídos e definidos os devidos tratamentos. Os riscos priorizados que possuem a maior relação impacto x probabilidade entrarão na zona do *heat map*, onde são discutidos e acompanhados bimestralmente no Comitê Executivo de Gestão de Riscos e Comitê de Auditoria, e, trimestralmente, nos Conselhos de Administração e Fiscal, ou em prazos inferiores, em caso de atualização material do *heat map* ou para tratar de assuntos específicos ou urgentes.

3.7 Papéis e responsabilidades

Conselho de Administração

- Deliberar sobre as questões estratégicas de Gestão de Riscos;
- Avaliar e aprovar o modelo de Gestão de Riscos e assegurar que este seja executado de acordo com a Política estabelecida;
- Avaliar e aprovar o grau de apetite a riscos e os limites das faixas de tolerância;
- Fornecer em bases periódicas, sua percepção quanto aos riscos tangíveis e intangíveis ao qual a Companhia está exposta;
- Avaliar e aprovar a Política de Gestão de Riscos.

Comitê de Auditoria

- Assessorar o Conselho de Administração nas questões relativas à Gestão de Riscos;
- Avaliar e monitorar as exposições a riscos da Companhia;
- Avaliar e supervisionar a efetividade e suficiência dos sistemas de gerenciamento dos riscos empresariais relevantes;
- Avaliar e supervisionar a conformidade da gestão para com as normas para assunção de riscos estabelecidas pela Companhia;
- Avaliar periodicamente o conjunto de padrões éticos, valores e atitudes da Companhia em relação aos riscos;
- Monitorar a qualidade e integridade dos sistemas de controles internos da Companhia e de suas controladas, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias

Conselho Fiscal

- Fiscalizar e avaliar os riscos prioritários;
- Fornecer em bases periódicas, sua percepção quanto aos riscos tangíveis e intangíveis.

Comitê Executivo de Gestão de Riscos

- Responsável final pelos riscos e sua gestão
- Validar o modelo, o portfólio de riscos e avaliações de riscos relevantes
- Implementar os modelos de Gestão dos Riscos;
- Priorizar recursos para assegurar adequada resposta aos riscos da Companhia;

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

- Aprovar as metas e ações para tratamento e mitigação dos riscos, dentro do apetite e limites estabelecidos pelo Conselho de Administração;
- Submeter ao Comitê de Auditoria os temas de Gestão de Riscos a serem propostos ao Conselho de Administração;

Diretor Vice-Presidente Financeiro

- É o responsável pela área de Gestão de Riscos na Companhia;
- Assegurar diretrizes, metas e que os recursos necessários sejam alocados para o bom funcionamento da área de Gestão de Riscos.

Diretorias

- O Diretor é o Responsável pelos Riscos de sua unidade de negócio.
- Asseguram a avaliação dos riscos e os planos de ação recomendados para mitigação dos riscos;
- Fornecem, em bases periódicas, sua percepção quanto aos riscos tangíveis e intangíveis ao qual suas respectivas áreas de negócio estão expostas;

Diretoria de Riscos

- Responsável por reportar os processos de Gestão de Riscos, diretamente ao Comitê de Auditoria.
- Acompanhar o modelo de Gestão de Riscos e assegurar que seja executado conforme metodologia definida para toda a empresa;
- Responsável por disseminar a cultura de riscos pela Companhia e/ou conhecimento específico para os colaboradores envolvidos no processo de gerenciamento de riscos;
- Obter e consolidar, entre os executivos, a percepção do grau de exposição aos riscos que a Eletropaulo está exposta;
- Coordenar e definir os padrões a serem seguidos no que tange o processo de Gestão de Riscos;
- Responsável por modelar e avaliar as exposições a riscos, com o objetivo de evidenciar e dar ciência sobre a magnitude de seus potenciais impactos;
- Assessorar as áreas de negócio na identificação/avaliação dos riscos, bem como na definição do plano de ação e contingência para tratamento dos riscos;
- Responsável pela supervisão dos controles e relatórios de risco das exposições aos fatores de riscos da Companhia, garantindo transparência na divulgação dos mesmos;
- Assegurar a manutenção da Política de Riscos, metodologia e portfólio de riscos da Eletropaulo;
- Avaliar periodicamente a maturidade do modelo de Gestão de Riscos adotado, indicando melhorias que assegurem uma evolução contínua deste modelo;
- Liderar o Comitê Executivo de Gestão de Riscos.

Responsável pelo Risco

- Definir o Gestor da Causa do Risco para tratamento dos riscos;
- Monitorar os riscos existentes em sua categoria de riscos e analisar tendências;
- Assegurar que os indicadores estão sendo atualizados de forma apropriada e monitorá-los;
- Validar planos de ação e assegurar que as ações necessárias estão sendo tomadas para minimizar a exposição da Companhia ao risco;
- Disponibilizar as informações necessárias para acompanhamento dos riscos pela área da Gerência de Riscos.

Gestor da Causa do Risco / Áreas de Negócio

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

- Conhecer o modelo de gerenciamento de riscos adotado pela Eletropaulo;
- Identificar, quantificar e propor adequado tratamento ao risco, contribuindo com o seu conhecimento técnico na análise dos riscos de negócio, na execução das atividades de controle e na elaboração dos planos de ação sempre que necessário;
- Obter a aprovação do (s) Diretor (es) aos planos de ação;
- Esclarecer eventuais dúvidas acerca de processos, leis, regulamentações e normas internas referentes à sua categoria de risco.

Auditoria Interna

- Supervisiona a governança de todo o processo de Gestão de Risco, bem como cumprimento das políticas, normas e procedimentos internos, em todos os seus níveis;
- Elabora o plano anual de auditoria, de forma independente, podendo considerar como parte da avaliação os subsídios fornecidos pela Gerência de Riscos.

3.8 Tipologia de Riscos

Os riscos da Eletropaulo são categorizados nos seguintes grupos:

Risco de Mercado

Relacionado possibilidade de perdas em posições financeiras e/ou físicas da Eletropaulo devido ao comportamento de fatores de mercado como preços, taxas de juros, taxas de câmbio, índices de inflação, etc.

Risco Estratégico

Representado pela falta de capacidade ou habilidade da Instituição em proteger-se, adaptar-se ou antecipar-se a mudanças que possam impedir o alcance dos objetivos corporativos estabelecidos e estratégias adotadas. Inclui o risco de: acompanhamento da gestão estratégica, frente à ausência da estratégia corporativa, dependência estratégica de pessoas, potencial desvio da missão e valores da Instituição, dissonância entre os objetivos estratégicos, táticos e operacionais, e dependência de fornecedores e terceiros.

Risco Regulatório e legal

Relacionado à possibilidade de perdas decorrentes de promulgação de novas regras ou de penalidades e indenizações resultantes do não cumprimento de obrigações regulatórias definidas pelos órgãos de supervisão e controle, bem como perdas decorrentes de decisão desfavorável em processos judiciais ou administrativos.

Risco Operacional

Decorrente da falta de consistência e adequação dos sistemas de informação, processamentos e controles das operações e geral da Eletropaulo.

Risco Compliance

Representado na possibilidade da Instituição não cumprir obrigações tais como conformidade com contratos, SLA's, OLA's, políticas corporativas e normativos internos, regulamentos, e códigos de conduta aplicáveis às suas atividades; bem como conduzir seus negócios com potenciais inobservâncias de requisitos aplicáveis aos novos projetos, serviços, soluções e mercados, podendo, conseqüentemente, causar danos à imagem e prejuízos de ordem financeira decorrentes de demandas judiciais e de sanções legais.

Risco Ambiental

Relacionado a possibilidade de danos ambientais devido a intervenção humana no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

Risco de Tecnologia

Representado pela perda resultante de falhas de sistemas, considerando tanto a infraestrutura quanto o processamento. Inclui o risco de haver potencial vazamento de informações, indisponibilidade e/ou fragilidades na infraestrutura de tecnologia da informação e ameaças de fraudes e/ou ataques cibernéticos.

Risco de Reputação e Imagem

Relacionado à possibilidade de perdas decorrentes ao desgaste da Eletropaulo junto ao mercado e/ou às autoridades, em razão de publicidade negativa, verdadeira ou não.

Risco Financeiro

Representado pela incerteza com relação às receitas e/ou custos devido às mudanças inesperadas no ambiente interno e/ou externo relacionada com suposições realizadas para fins de planejamento e que resulte na incapacidade da operação dos sistemas da Instituição de cumprir seus compromissos financeiros. Podem ter origem contábil, atuarial, fiscal, liquidez e etc.

4. REFERÊNCIAS

COSO ERM – Enterprise Risk Management 2004

ISO 31000 – Gestão de Riscos

Benchmarks de melhores práticas do mercado e diretrizes CVM

5. DEFINIÇÕES

Risco

É o efeito da incerteza nos objetivos estratégicos da organização. Esta incerteza pode ser reconhecida e identificada de maneira positiva quando for uma oportunidade, ou de maneira negativa quando tratar-se de uma ameaça.

Evento

É o fato ou acontecimento que caracteriza a materialização do risco. Pode consistir de uma ou mais ocorrências e ter várias causas diferentes. Pode também consistir da não ocorrência de algum fato ou acontecimento. Pode também ser referido algumas vezes como um "incidente" ou "acidente".

Apetite a Risco

Quantidade e tipo de riscos que uma organização está preparada para buscar, manter e assumir.

Impacto/ Probabilidade

Impacto é a extensão a que a Companhia pode estar exposto ou desprotegido com relação aos eventos negativos e seus efeitos, antes e/ou depois da avaliação do respectivo risco, podendo ser de ordem tangível ou intangível.

Probabilidade é possibilidade/chance de materialização do risco considerando a atual estrutura de controles da Companhia: técnicas atuais para mitigação de riscos, eficiência e eficácia de controles, histórico e impactos anteriores de riscos, complexidade do gerenciamento de riscos e nível de crescimento e contração.

POLÍTICA DE GESTÃO DE RISCOS - ELETROPAULO

Riscos Prioritários

Grupo de riscos com impacto potencialmente elevado para o negócio, cuja gestão deve ser priorizada e seus indicadores devem ser monitorados regularmente.

Responsável pelo Risco

O responsável pelo risco é a pessoa ou entidade que foi dada a autoridade para gerenciar e/ou delegar risco(s) em particular.