POLÍTICA DE GESTÃO DE RISCOS

1 - Disposições Preliminares

A presente "Política de Gestão de Riscos", tem como objetivo estabelecer as diretrizes e responsabilidades na gestão de riscos da Nuclebrás Equipamentos Pesados S/A – NUCLEP, especialmente no tocante à identificação e análise dos riscos que possam afetar a empresa, bem como estabelecer controles e procedimentos para monitoramento, de forma a diminuir as probabilidades de ocorrência de riscos ou minimizar seus impactos.

2 - Abrangência

Este Documento Normativo aplica-se a todos os Macroprocessos e Operações de Negócios da NUCLEP.

3 - Definições

3.1 - Ação de contingenciamento: ação ou conjunto de ações que têm por objetivo contornar a situação anormal após ocorrência de um evento de risco;

3.2 - Ação de resposta a riscos: ação ou conjunto de ações que têm por objetivo a diminuição da probabilidade da ocorrência e/ou impacto de um evento de risco;

3.3 - Alta administração: Presidente, Diretor Administrativo, Diretor Comercial e Diretor Industrial;

3.4 - Apetite ao risco: disposição da organização em suportar o risco após o tratamento, resposta e contingenciamento, a fim de atingir sua missão e objetivos estratégicos;

3.5 - Atividade: conjunto de tarefas essenciais que determinam a entrega de uma parte específica e definível de um produto ou serviço de um processo;

3.6 - Atividades de controles internos: atividades materiais e formais, como políticas, instruções, técnicas, procedimentos, ferramentas e práticas, implementadas pela gestão de modo a diminuir riscos organizacionais e assegurar o alcance de objetivos da gestão;

3.7 - Categoria de Risco: definição de tipo de evento de risco baseado no *framework COSO,* podendo ser:

3.7.1 - Estratégico;

3.7.2 - Integridade

3.7.3 - Comunicação;

3.7.4 - Operacional.

3.8 - Causa: fatores que podem desencadear um evento de risco;

3.9 - Ciclo de gestão de riscos: período de tempo em que são realizadas as atividades de gestão de riscos organizacionais;

3.10 - Consequência: efeitos decorrentes do acontecimento de um evento de risco;

3.11 - Controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de colaboradores da organização, destinados a enfrentar os riscos organizacionais de modo que, na consecução da missão da entidade, os objetivos da gestão sejam alcançados;

3.12 - Cultura de gestão de risco: valores, princípios, conceitos éticos e crenças que existem na organização e interagem com as estruturas da organização e sistemas de controle, de modo a produzir normas de comportamento que são favoráveis aos objetivos de gestão de riscos;

3.13 - Estratégia de resposta a riscos: definição de ações estruturadas que objetivam o direcionamento da elaboração de ações de resposta para determinado risco, podendo ser:

3.13.1 - Aceitar: situação em que nenhuma medida pode ser efetivamente tomada para levar o risco a um estado melhor, quer seja por um fator que foge do controle da companhia quer seja por ser impraticável a diminuição da probabilidade de sua ocorrência e/ou do impacto;

3.13.2 - Dividir: situação em que são tomadas medidas de modo a reduzir o impacto advindo de sua ocorrência, através de ações que compartilhem parte da responsabilidade e consequências;

3.13.3 - Eliminar: situação em que o evento de risco for passível de sofrer uma interferência direta da empresa que elimine completamente sua probabilidade de ocorrência e/ou os impactos advindos da ocorrência deste evento de risco;

3.13.4 - Mitigar: situação em que são tomadas medidas para reduzir a probabilidade de ocorrência do evento de risco e/ou o impacto advindo da sua ocorrência; e

3.13.5 - Transferir: situação em que são tomadas medidas para eliminar o impacto de um evento de risco, executando a transferência total das consequências para uma segunda parte, fazendo-a responsável pela execução de atividade que gere evento de risco e/ou responsável pelos impactos da ocorrência do evento.

3.14 - Evento de risco: fato que desencadeia a materialização de um risco;

3.15 - Função de risco: setor com responsabilidade de gestão de riscos, integrantes da segunda linha de defesa;

3.16 - Gestão de riscos: conjunto de normativos externos, normativos internos, princípios, estruturas, processos e atividades coordenados de gestão e controle da organização no que se refere à gestão de riscos;

3.17 - Gestores: integrantes da primeira linha de defesa e responsáveis por supervisionar a gestão de riscos pelo setor que executa os processos;

3.18 - Impacto: graduação da gravidade dos efeitos de um evento de riscos que pode influenciar na realização de um objetivo;

3.19 - Método de Gestão de Riscos: técnicas, regras e procedimentos que definem a forma de execução da gestão de riscos;

3.20 - Plano de Ação: conjunto de atividades com o objetivo de alcançar a estratégia de resposta a riscos, de forma a diminuir suas probabilidades de ocorrência e/ou seus impactos;

3.21 - Plano de Contingenciamento: conjunto de atividades com o objetivo de minimizar os danos causados pela ocorrência dos riscos quando o plano de ação não é eficaz e/ou o evento de risco;

3.22 - Probabilidade: graduação da possibilidade de ocorrência ou não de um evento de riscos que pode influenciar na realização de um objetivo;

3.23 - Processo: conjunto de atividades que têm por objetivo produzir um ou mais resultados;

3.24 - Programa de gestão de riscos: sistematização de processos, procedimentos e metodologias para o desenvolvimento, a implementação, o monitoramento, a manutenção e a melhoria contínua da gestão de riscos;

3.25 - Proprietário do risco: unidade organizacional pela identificação de seus riscos;

3.26 - Riscos: são fatores ou eventos incertos, externos ou internos, que possuem certa probabilidade de ocorrência e podem causar impactos no cumprimento dos objetivos estratégicos da NUCLEP;

3.27 - Riscos estratégicos: são os riscos que influenciam os objetivos estratégicos, alinhados com a missão/visão da organização, impactando diretamente na forma de geração de valor definida pela alta administração, como por exemplo: riscos políticos, econômicos, sociais, ambientais, legais, tecnológico, de imagem, financeiros/orçamentários, dentre outros;

3.28 - Riscos de integridade: são os riscos que se relacionam com o cumprimento de leis, regulamentos e normativos internos e externos, como por exemplo: aderência a normativos, segregação de funções, conduta profissional inadequada, ameaça à imparcialidade e à autonomia técnica, uso indevido de autoridade, nepotismo, conflito de interesses, uso indevido ou manipulação de dados/informações, desvio de pessoal ou de recursos materiais, corrupção, fraude e emprego irregular de

verbas públicas, não conformidade com normativos internos, não conformidade com normativos externos, não cumprimento do princípio de segregação de funções.

3.29 - Riscos de comunicação: são os riscos relacionados à forma, qualidade e prazo em que as informações relevantes são identificadas, colhidas, tratadas e transmitidas, como por exemplo: falhas de processos de comunicação interna, comunicação externa, comunicação com partes interessadas;

3.30 - Riscos operacionais: são os riscos decorrentes da inadequação ou falha nos processos internos, que possam dificultar ou impedir o alcance dos objetivos estratégicos da empresa, como por exemplo: riscos de processos, certificações, termos de referência, propostas, dentre outros. Estes riscos estão associados tanto ao processo industrial como à gestão de áreas administrativas; e

3.31 - Unidades organizacionais: Gerências, Gerências Gerais, Diretorias e Assessorias.

4 - Princípios

4.1 - Criar e proteger valor;

4.2 - Ter o compromisso da alta administração com a gestão de riscos eficaz, que permeia toda a instituição;

4.3 - Ser parte integrante de todos os processos organizacionais incluindo o Plano de Negócios e Planejamento Estratégico;

4.4 - Ter o compromisso de todos os colaboradores com a aderência às normas;

4.5 - Ser sistemática, estruturada, oportuna, dinâmica, transparente, inclusiva, interativa e capaz de reagir às mudanças;

4.6 - Proceder a tomada de decisão pautada na análise e gestão dos riscos;

4.7 - Abordar as incertezas visando gerenciar os riscos da NUCLEP;

4.8 - Estabelecer procedimentos de controles internos proporcionais aos riscos de integridade, observado o apetite do risco e a relação custo-benefício destinados a agregar valor à NUCLEP;

4.9 - Estar alinhada com o contexto interno e externo da NUCLEP;

4.10 - Considerar fatores humanos e culturais que possam impactar na realização dos objetivos da NUCLEP; e

4.11 - Contribuir para melhoria contínua da NUCLEP.

5 - Diretrizes

5.1 - Alinhar as ações de gerenciamento de riscos aos princípios e objetivos organizacionais, **tendo total autonomia para decidir quais tipos e categorias de riscos podem e devem ser gerenciados dentro da empresa, de acordo com a natureza, complexidade, nível de risco, probabilidade e impacto da ocorrência, e das necessidades das operações que forem realizadas.**

5.2 - Observar a missão, a visão, os valores, os objetivos e o planejamento estratégico da instituição;

5.3 - Observar as competências e as atribuições regimentais das unidades que compõem a NUCLEP;

5.4 - Identificar e tratar os riscos de negócio e operacionais de forma a garantir o cumprimento das metas estabelecidas em seu plano de negócios e planejamento estratégico;

5.5 - Identificar e avaliar os riscos de acordo com a probabilidade de ocorrência e seu impacto sobre o negócio, inclusive, sobre a imagem da empresa;

5.6 - Disseminar as informações necessárias ao fortalecimento da cultura de gestão de riscos;

5.7 - Basear decisões tomadas levando em consideração os benefícios, os aspectos negativos e os riscos atrelados, mensurando a relação entre a probabilidade, impacto, resposta a risco e contingenciamento;

5.8 - Promover, por meio da avaliação de riscos, a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos;

5.9 - Considerar prioridades estratégicas definidas pelo órgão para o planejamento da gestão de riscos organizacionais;

5.10 - Medir o desempenho da gestão de riscos organizacionais na NUCLEP por meio do nível de risco apurado nos seus processos; e

5.11 - Fomentar o desenvolvimento contínuo dos colaboradores da NUCLEP para o processo de gerenciamento de riscos.

6 - Objetivos

6.1 - Subsidiar a elaboração do planejamento estratégico institucional e seu plano de negócios, seus desdobramentos e a cadeia de valor;

6.2 - Contribuir para a melhoria contínua do desempenho dos processos e das políticas da organização no que tange gestão de riscos;

6.3 - Executar periodicamente as etapas que compõem o processo de gerenciamento de riscos;

6.4 - Utilizar-se de metodologia, ferramentas e conhecimento para o apoio à gestão de riscos convergentes com o *framework COSO,* a ISO 31000:2018 e outras melhores práticas;

6.5 - Promover o desenvolvimento contínuo dos agentes em gestão de riscos;

6.6 - Estabelecer responsabilidades e competências para os agentes envolvidos no processo de gestão de riscos;

6.7 - Estabelecer níveis adequados de exposição e apetite a riscos;

6.8 - Promover a cultura de gestão de riscos na NUCLEP;

6.9 - Obter segurança razoável no cumprimento das obrigações de gestão de riscos;

6.10 - Gerar informações tempestivas relacionadas à conformidade para que auxiliem a gestão na tomada de decisão; e

6.11 - Promover uma abordagem abrangente da gestão de riscos, integrando-a com a estratégia organizacional, a gestão de riscos, controles internos, os princípios éticos e os princípios gerais de governança;

7 - Responsabilidades e Competências

7.1 - Conselho de Administração aprova metodologias de gestão de riscos, normas necessárias à efetivação do sistema, aprova o apetite e a tolerância a riscos da empresa, através dos direcionadores estratégicos e orientação geral, assegura e a efetividade do sistema de controle de riscos e oferece suporte necessário para sua efetiva implementação;

7.2 - Diretoria Executiva estabelece a estratégia da empresa e da estrutura de gestão de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão, além de emitir e monitorar recomendações para o aprimoramento da governança e da gestão de riscos na instituição, supervisionando a adoção de providências para responder aos riscos que possam comprometer o cumprimento dos objetivos estratégicos;

7.3 - Área de Gestão de Riscos gerencia e supervisiona as atividades de gestão de riscos estratégicos, operacionais e de comunicação, divulga práticas eficazes de gerenciamento de riscos e monitora a implementação pelas unidades organizacionais no devido cronograma e escopo;

7.4 - Comitê de Governança, Riscos e Controle identifica os riscos de conformidade, operacionais da Área de Gestão de Riscos e respectivos controles internos destes processos, garantindo assim o cumprimento do princípio de segregação de funções;

7.5 - Proprietário de Risco deve assegurar que os riscos sejam levantados de acordo com a presente política e normativos internos, monitorar os riscos ao longo do tempo, executar as ações de resposta aos riscos e as ações de contingenciamento caso aplicáveis, garantir informações adequadas sobre os riscos estejam disponíveis prontamente para a Área de Gestão de Riscos durantes as respectivas fases do ciclo de gestão de riscos; e

7.6 - Colaboradores da NUCLEP devem respeito às previsões desta Política e dos normativos internos, sendo responsáveis pelo seu cumprimento.

8 - Instrumentos

8.1 - Manual de Fluxo de Processo de Gerir Riscos Organizacionais;

8.2 - Manual de Fluxo de Processo de Gerir Riscos Operacionais;

8.3 - Manual de Fluxo de Processo de Gerir Riscos Estratégicos;

8.4 - Manual de Fluxo de Processo de Gerir Riscos de Comunicação;

8.5 - Manual de Fluxo de Processo de Gerir Riscos de Integridade;

8.6 - Método de Gestão de Riscos;

8.7 - Plano de capacitação em gestão de riscos;

8.8 - Orientações, recomendações e procedimentos de gestão de Integridade;

8.9 - Códigos de ética e conduta da instituição; e

8.10 - Relatórios de monitoramento e controles internos.

9 - Disposições Finais

Os casos omissos relativos a esta Política serão submetidos ao Conselho de Administração.

A revisão deste documento se dará no mínimo a cada triênio.

A revisão dos riscos, planos de ação e planos de contingenciamento se dará pelo menos anualmente, dentro de cada exercício fiscal.

A política será tempestivamente divulgada aos colaboradores e administradores da NUCLEP.

O treinamento relativo a essa política será ministrado anualmente aos administradores da empresa.

A presente Política foi avaliada e aprovada pelo Conselho de Administração Nuclebrás Equipamentos Pesados S.A. - NUCLEP conforme Ata 156ª do CA, item 07, de 18/05/2022.

Itaguaí, 18 de maio de 2022.

Histórico de Revisões

Primeira Versão: aprovada na 110ª Reunião do Conselho de Administração, realizada em 25/06/2018.

Segunda Versão: aprovada na 123ª Reunião do Conselho de Administração, realizada em 20/09/2019.

Terceira Versão: aprovada na 140ª Reunião do Conselho de Administração, realizada em 22/02/2021.