POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS DA ELETRONUCLEAR S/A

Versão 06

Eletronuclear
Energia Limpa

Política de Gestão de Riscos e Controles Internos da Eletronuclear

Área responsável pela emissão

Presidência / Superintendência de Processos, Gestão de Riscos e Conformidade

Público-Alvo

Membros da Alta Administração, dos Comitês Estatutários, gestores e demais colaboradores da Eletronuclear.

Aprovação

Resolução 1780.003/24, de 14/05/2024, da Diretoria Executiva da Eletronuclear.
Deliberação 538.002/24, de 27/05/2024, do Conselho de Administração da Eletronuclear.

Repositório

As políticas da Eletronuclear podem ser encontradas no *site*:
https://etnweb.sharepoint.com/sites/Documentacao/PoliticasCorporativas/Forms/AllItems.aspx

Prazo máximo de revisão: 3 anos

Histórico de Versões

Versão	Aprovação	Principais alterações
1	29/04/2011	Não se aplica.
2	30/10/2014	Ampliação do escopo, de forma a englobar as atividades relativas a controles internos e à Certificação SOX.
3	23/09/2016	Adequação ao *framework* COSO 2013 e à Lei nº 12.846/2013.
4	26/09/2019	Adequação à Norma ISO 31000:2018, à Lei nº 13.303/2016 e ao Decreto nº 8.945/2016.
5	18/06/2021	Adequação ao COSO ERM 2017, ao Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC 2015 e ao Modelo das Três Linhas do IIA 2020.
6	RDE-1780.003/24, de 14/05/2024. DCA-538.002/24 de 27/05/2024	Exclusão das referências à Eletrobras, devido ao evento de capitalização. Referências: exclusão de referências ao Decreto nº 8.420/2015, ao Documento *Sarbanes-Oxley Act*/2002 e à Instrução CVM 480/2009, e inclusão de referências às Leis nº 13.709/2018 (LGPD), nº 14.230/2021

		e nº 14.133/2023, ao Decreto nº 11.129/2022, ao Manual de Gestão de Riscos do TCU/2020 e à Norma CNEN-NE-1.26. Princípios: adição de tópicos referentes a declaração de tolerância a riscos, de treinamento acerca de gestão de riscos e de segurança nuclear. Diretrizes: adequação das etapas da gestão de riscos à nova metodologia adotada. Responsabilidades: adição das responsabilidades do Comitê de Auditoria e Riscos – COAUD, das áreas proprietárias dos Riscos de Segurança Nuclear, da Coordenação de Segurança e Supervisão Independente e do Comitê de Riscos e Segurança Nuclear.

Sumário

1 Objetivo

Estabelecer princípios, diretrizes e responsabilidades para processo de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos às atividades da Eletronuclear, promovendo uma cultura de gerenciamento de riscos que agregue valor, incorporando-a ao seu planejamento estratégico e à tomada de decisões, em conformidade com as regulamentações aplicáveis e com as melhores práticas de mercado.

2 Referências

2.1 Lei Federal nº 8.429/1992 (Lei da Improbidade Administrativa) – dispõe sobre as sanções e dá outras providências.

2.2 Lei Federal nº 14.230, de 25 de outubro de 2021, que altera a Lei 8.429/1992 (LIA).

2.3 Lei Federal nº 12.846/2013 (Lei Anticorrupção) – dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.

2.4 Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2.5 Lei Federal nº 13.303/2016 (Lei das Estatais) – dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

2.6 Decreto Federal nº 11.129/2022 – regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.

2.7 Decreto nº 8.945/2016 – regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

2.8 Lei Federal nº 14.133, de abril de 2023 – Licitações e contratos administrativos.

2.9 *Foreign Corrupt Practices Act* (FCPA), 1977.

2.10 COSO 2013 (*Committee of Sponsoring Organizations of the Treadway Commission) – Internal Control – Integrated Framework*.

2.11 Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC, 2023.

2.12 COSO ERM 2017 *(Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*).

2.13 Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes.

2.14 Modelo das Três Linhas do IIA 2020 – uma atualização das Três Linhas de Defesa (*Institute of Internal Auditors*).

2.15 Manual de Gestão de Riscos do TCU – 2º edição – Brasília, 2020.

2.16 Norma CNEN-NE-1.26 – Segurança na operação de Usinas Nucleoelétricas.

3 Princípios

3.1 Declaração de Apetite a Riscos

A criação de valor é essencial para a Eletronuclear. A liderança em nosso mercado por meio de investimentos em Geração focados em energia limpa é parte de nossa proposta de expansão sustentável. A declaração de apetite a riscos será estabelecida com base em metodologia interna com aprovação de alçada competente.

3.2 Declaração de Tolerância a Riscos

Não toleramos riscos que possam comprometer a segurança operativa das usinas e de nossos ativos, a saúde e segurança de nossos colaboradores, a sustentabilidade empresarial e socioambiental, como também a rentabilidade, disciplina financeira e os padrões éticos e de Compliance.

3.2.1 A Eletronuclear atuará na gestão de riscos sob princípios e procedimentos alinhados a suas responsabilidades em temas como governança corporativa, ambiental e social (ESG).

3.3 Treinamentos acerca de Gestão de Riscos

A Eletronuclear deverá elaborar plano de comunicação e treinamento para abranger todos os colaboradores de acordo com o grau de participação de suas atividades em funções que tangem a Gestão de Riscos.

3.4 Geração de valor para a empresa

A Eletronuclear reconhece que a gestão integrada de riscos corporativos está diretamente relacionada às diretrizes estratégicas de crescimento sustentável, rentabilidade e criação de valor para a empresa, por permitir a identificação preventiva de ameaças aos objetivos de negócio e a tomada de decisões baseada em riscos.

3.5 Adoção de boas práticas de governança corporativa

A Eletronuclear busca adotar as melhores práticas de governança corporativa, no que tange à gestão de riscos e a políticas e práticas antifraude e anticorrupção, de forma sistemática, estruturada e oportuna, com o intuito de aprimorar e manter a transparência e a qualidade das suas informações, divulgadas interna e externamente, buscando melhor reputação perante o mercado e um diferencial na geração de valor para os seus acionistas e demais partes interessadas.

3.6 Definição de linguagem comum para a gestão de riscos

A adoção de uma linguagem padrão para a gestão de riscos na empresa é essencial ao processo, possibilitando melhor entendimento entre as partes e uma comunicação livre de interferências.

3.7 Utilização de padrões e metodologias reconhecidos pelo mercado

Com um modelo baseado em metodologias e padrões formalizados, reconhecidos pelo mercado e disseminados na Eletronuclear, a gestão integrada de riscos está alinhada às estratégias, iniciativas e estruturas organizacionais, além de atender às exigências setoriais e dos órgãos reguladores e fiscalizadores.

3.8 Estabelecimento de papéis e responsabilidades

A Eletronuclear define e comunica formalmente os papéis e as responsabilidades de cada um dos colaboradores envolvidos no processo de gestão de riscos.

3.9 Envolvimento dos órgãos de governança

As atuações do Conselho de Administração, do Comitê de Auditoria e Riscos – COAUD – responsáveis por deliberar sobre gestão de riscos, e da Diretoria Executiva assumem papel primordial para o sucesso da gestão de riscos, uma vez que são esses os principais envolvidos nas tomadas de decisão sobre questões estratégicas da empresa.

3.10 Estabelecimento e manutenção da infraestrutura necessária para a gestão integrada de riscos

Para gerenciar os riscos de forma eficiente, a Eletronuclear busca possuir uma infraestrutura adequada e integrada de processos, pessoas e tecnologia, estabelecendo mecanismos de comunicação claros e objetivos.

3.11 Integração da gestão de riscos aos processos organizacionais

A gestão integrada de riscos deve permear todas as práticas e processos organizacionais da Eletronuclear, de forma a garantir a identificação de eventos de riscos inerentes a todas as suas áreas de negócio.

3.12 Análise periódica da gestão de riscos

A Eletronuclear deve assegurar a eficácia do gerenciamento de riscos por meio de revisões frequentes, favorecendo o cumprimento de seus objetivos e avaliando sua maturidade em gestão de riscos, por meio de um modelo adaptado do Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC.

3.13 Adoção do modelo das Três Linhas

A Eletronuclear adota o modelo de gestão de riscos baseado nos conceitos das três linhas, sendo:

- Primeira linha: Superintendências e áreas de negócios, além dos gestores de projetos e de processos. Esta linha é responsável pela provisão de produtos/serviços aos clientes e por gerenciar riscos;

- Segunda linha: Áreas de riscos e de Controles Internos. Tem o papel de fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, e também de fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos;

- Terceira linha: Auditoria Interna. Esta linha realiza avaliação e assessoria independentes e objetivas sobre questões relativas ao atingimento dos objetivos.

3.14 Segurança Nuclear

A segurança nuclear é prioritária. A Eletronuclear tem na segurança um dos pontos mais relevantes de sua cultura organizacional, norteando todas as atividades da empresa, mesmo as que, aparentemente, nada tem a ver com a questão.

4 Diretrizes

4.1 Identificação dos riscos

4.1.1. A identificação de riscos deve reconhecer e descrever os riscos aos quais a empresa está exposta, considerando inclusive as possíveis alterações em seu ambiente de negócios.

4.1.2. O objetivo desta etapa é identificar eventos que interferem potencialmente no plano estratégico da Companhia.

4.2 Análise dos riscos

4.2.1. A análise do risco se refere ao desenvolvimento da compreensão sobre o risco e à determinação do nível do risco.

4.2.2. O grau de exposição do risco deverá ser graduado em cinco níveis, definidos com base na análise de impacto e probabilidade.

4.2.3. Os riscos são classificados e categorizados em uma linguagem comum, considerando suas respectivas características.

4.3 Avaliação dos riscos

4.3.1 A avaliação do risco envolve a comparação do seu nível com o limite de exposição a riscos, a fim de determinar se o risco é aceitável.

4.4 Tratamento dos riscos

4.4.1. Compreende o planejamento e a realização de ações para modificar o nível do risco. O nível do risco pode ser modificado por meio de medidas de respostas aos riscos que incluem mitigar, transferir, evitar ou aceitar o risco.

4.4.2. A Eletronuclear terá definição dos níveis de tolerância ao risco, indicando os níveis que requeiram ou não ações específicas para sua mitigação.

4.5 Monitoramento dos Riscos

4.5.1. Compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

4.5.2. Os riscos poderão ser monitorados mediante Indicadores Chave de Riscos (KRI) de modo a possibilitar a identificação quantitativa de sua ocorrência.

4.6 Comunicação dos riscos

4.6.1. A comunicação, durante todas as etapas do processo de gestão de riscos, deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado.

4.6.2. Os donos dos riscos são responsáveis por compartilhar tempestivamente e de forma proativa quaisquer novidades e/ou potenciais riscos que impactem o negócio ao departamento responsável pela gestão de riscos da Eletronuclear.

4.7 Identificação de Controles

4.7.1. Uma das etapas da gestão de riscos consiste na identificação de respostas aos riscos e sua atualização constante, no intuito de garantir que a estrutura de controles internos da Eletronuclear esteja adequada aos desafios e constantes melhorias sofridas pela empresa e suas operações.

4.8 Avaliação do Desenho do Controle

4.8.1. Após a identificação e descrição dos controles, os mesmos devem ser avaliados para confirmar se, conceitualmente, eles estariam mitigando os riscos aos quais estão relacionados. Essa avaliação pode ser realizada através de um procedimento chamado walkthrough de controle, que consiste na análise de uma ocorrência do controle em questão.

4.9 Testes da Administração

4.9.1. Os auditores internos desempenham uma função essencial ao avaliar a eficácia dos controles internos e ao recomendar melhorias para estes.

4.10 Remediação

4.10.1. A remediação das deficiências, realizada pelos responsáveis pelos controles, com o apoio do Departamento de Gestão de Riscos e Controles Internos, visa à elaboração de planos de ação para solução das deficiências apontadas nos Testes da Administração.

5 Responsabilidades

5.1 Conselho de Administração

5.1.1. Aprovar a política de gestão de riscos, a matriz de riscos, a priorização de riscos e o cronograma de reporte de riscos, bem como suas revisões.

5.1.2. Aprovar o apetite ao risco da Eletronuclear.

5.1.3. Supervisionar o processo de gestão de riscos por meio de reportes regulares da Diretoria Executiva, com foco na assertividade do processo e nas respostas aos riscos.

5.2 Comitê de Auditoria e Riscos - COAUD

5.2.1. Assessorar o Conselho de Administração em todas as matérias relacionadas à avaliação e gerenciamento de riscos.

5.2.2. Supervisionar as atividades da unidade organizacional da Empresa responsável pela gestão de riscos e controles internos.

5.2.3. Avaliar e monitorar a exposição ao risco da empresa estatal e requerer, entre outras, informações detalhadas sobre políticas e procedimentos referentes à remuneração da administração, à utilização de ativos da Empresa e aos gastos incorridos em nome da empresa estatal.

5.2.4. Supervisionar o mapeamento e a avaliação dos riscos que podem comprometer a empresa.

5.2.5. Solicitar parecer de risco à área responsável quando julgar necessário.

5.2.6. Propor ao Conselho de Administração da Eletronuclear, a aprovação da Política de Gestão de Riscos implementada na Empresa, inclusive suas futuras alterações, seus princípios, conceitos, seu método de operacionalização e posteriores alterações.

5.2.7. Avaliar relatórios destinados ao Conselho de Administração que tratem de controles internos relacionados a aspectos financeiros, contábeis, operacionais, legais e éticos, elaborados pela auditoria interna e pelas unidades organizacionais responsáveis pelas avaliações destes controles, e verificar o cumprimento das recomendações contidas nesses relatórios.

5.3 Conselho Fiscal

5.3.1. Contribuir sobre o tema, fazendo constar de suas atas as informações complementares que julguem necessárias ou úteis ao processo de gestão de riscos.

5.4 Diretoria Executiva

5.4.1. Avaliar a assertividade do processo de gestão de riscos por meio dos reportes periódicos, discutindo e validando, no colegiado ou por diretoria, as avaliações apresentadas pelas áreas proprietárias de riscos e definindo o posicionamento frente aos riscos, de acordo com o apetite aprovado pelo Conselho de Administração.

5.4.2. Assegurar a implantação da gestão de riscos na empresa, alocando recursos necessários ao processo e definindo a infraestrutura apropriada às atividades de gerenciamento de riscos.

5.4.3. Aprovar normas específicas.

5.4.4. Aprovar a definição das áreas proprietárias de riscos.

5.4.5. Propor a aprovação da matriz de riscos, a priorização de riscos e o cronograma de reporte de riscos, bem como suas revisões, encaminhando-os para aprovação do Conselho de Administração.

5.5 Área de Gestão de Riscos Corporativos

5.5.1. Atuar como segunda linha, coordenando e definindo os padrões a serem seguidos, no que tange aos processos de gestão de riscos, aos seus sistemas de suporte e às formas e à periodicidade de seus reportes.

5.5.2. Apoiar e garantir o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento e o monitoramento dos riscos corporativos da Eletronuclear, bem como consolidar e reportar a situação dos riscos priorizados para a Diretoria Executiva, COAUD e ao Conselho de Administração, incluindo os riscos de alto nível relativos à segurança nuclear.

5.5.3. Disseminar a cultura de gestão de riscos e controles internos na empresa.

5.5.4. Monitorar o grau de exposição do risco com base nos KRIs definidos.

5.5.5. Prestar apoio nas atividades do Comitê de Gerenciamento de Riscos de Segurança Nuclear, relativo ao gerenciamento de riscos em alto nível da segurança nuclear.

5.6 Áreas Proprietárias de Riscos

5.6.1. Atuar como primeira linha, gerenciando os riscos operacionais inerentes às suas atividades, identificando-os, avaliando-os, tratando-os e monitorando-os, em especial os riscos de operação das usinas.

5.6.2. Prover a Área de Riscos Corporativos de todas as informações necessárias, com solidez e fidedignidade.

5.6.3. Comunicar tempestivamente e de forma proativa quaisquer novidades e/ou potenciais riscos que impactem o negócio ao departamento responsável pela gestão de riscos da Eletronuclear;

5.6.4. Reportar ao Comitê de Riscos de Segurança Nuclear os resultados das análises dos riscos operacionais das usinas.

5.7 Áreas Proprietárias de Riscos de Segurança Nuclear

5.7.1. Superintendência de Coordenação da Operação

5.7.1.1. Coordenar e assegurar, em conjunto com as Superintendências das Usinas de Angra 1 e 2, a efetiva identificação, análise, avaliação e tratamento dos riscos de segurança nuclear.

5.7.1.1.1. Exercer o papel de *risk owner* dos riscos identificados nos processos de operações das usinas.

5.7.2. Superintendências de Angra 1 e 2

5.7.2.1. Atuar na identificação dos riscos de seus processos e como responsável pela operacionalização das respostas de mitigação e dos planos de contingência dos riscos identificados nos processos de operações das usinas.

5.7.2.1.1 Exercer o papel de *control owner* dos riscos identificados nos processos de operações das usinas.

5.7.3. Superintendência de Engenharia de Apoio à Operação

5.7.3.1. Prestar apoio no processo de gerenciamento de riscos de segurança nuclear junto às Superintendências de Coordenação e Operação e às Superintendências das Usinas de Angra 1.

5.8. Coordenação de Segurança e Supervisão Independente

5.8.1 Coordenar, em conjunto com as demais Unidades Organizacionais da empresa, as ações necessárias à integração do conceito de segurança, incluindo a nuclear.

5.8.2 Instituir e coordenar o Programa de Observação Independente e Avaliação de Cultura de Segurança no Campo, incluindo áreas de operação das usinas.

5.8.3 Supervisionar de forma independente a eficácia do gerenciamento dos riscos relacionados à operação segura e confiável das usinas.

5.9 Comitê de Riscos de Segurança Nuclear

5.9.1 Exercer a análise e a supervisão de todos os processos de gerenciamento de riscos relacionados à Segurança Nuclear.

5.9.2. Integrar o gerenciamento dos riscos operacionais de segurança nuclear realizado pelas áreas proprietárias dos riscos.

5.9.3 Reportar periodicamente à alta administração, os resultados das análises dos riscos operacionais das usinas com maior grau de exposição (nível alto e muito alto).

5.9.4 O Comitê será formado ao menos pelos titulares das seguintes unidades organizacionais: CS.DE, DGC.P, SC.O, SU.O, SD.O, SO.T e DAS.T.

6 Conceitos

6.1 Apetite ao risco – limite de exposição aos riscos que a empresa está disposta a aceitar para atingir seus objetivos estratégicos e criar valor para os acionistas.

6.2 Área proprietária de risco (*Risk Owner*) – unidade organizacional que possui autoridade e responsabilidade pelo gerenciamento do risco.

6.3 Gestão integrada de riscos – arquitetura implantada na Eletronuclear para gerenciamento de riscos, sob metodologia e linguagem comuns, alinhada com as demais linhas; a gestão integrada de riscos, por meio de um enfoque estruturado e da melhor compreensão das inter-relações entre riscos, alinha estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e a criação de valor para a empresa e seus acionistas.

6.4 Impacto – resultado da materialização de um risco que afeta processos e objetivos de negócio da empresa, podendo ser expresso de forma qualitativa ou quantitativa.

6.5 Nível de Risco – medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e seu impacto nos objetivos.

6.6 Matriz de Riscos – conjunto dos eventos de risco identificados pela empresa, descritos e classificados em categorias.

6.7 Modelo das Três Linhas – consiste em um conjunto de princípios e diretrizes, elaborado e divulgado pelo IIA Global, *The Institute of Internal Auditors*, que visa esclarecer e organizar as responsabilidades e papéis dos profissionais da organização no gerenciamento de riscos e controles.

6.8 Probabilidade – chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente.

6.9 **Resposta ao Risco** – ação para mitigar, transferir, evitar ou aceitar a exposição da empresa ao risco, atuando na probabilidade e/ou no impacto, incluindo, mas não se limitando a, controles internos.

6.10 **Risco** – Evento incerto que, em caso de ocorrência, provocará um impacto positivo ou negativo no alcance dos objetivos.

6.11 **Objeto de gestão de riscos (objeto de gestão)** – qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos da empresa.

6.12 **Riscos Corporativos** – são riscos com potencial de afetar, de forma relevante, o atingimento dos objetivos estratégicos da empresa.

6.13 **Controles Internos -** estruturados para oferecer segurança razoável de que os objetivos da organização sejam alcançados e a empresa fique mais protegida de eventos indesejados que possam causar prejuízos pecuniários ou danos à sua imagem.

7 Disposições Gerais

7.1 Esta política está alinhada com as demais políticas da Eletronuclear.

7.2 A Eletronuclear deve garantir que os princípios e diretrizes estabelecidos nesta política sejam seguidos por todos.

7.3 O presente documento deve ser considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes, adotados pela Eletronuclear, em particular aqueles relacionados a fraudes, corrupção e conduta antiética.

7.4 As exceções, eventuais violações e casos omissos a esta política devem ser submetidos à apreciação da Superintendência de Processos, Riscos e Conformidade, e encaminhados para posterior aprovação dos órgãos competentes.