www.revistaft.com.br

Revista FT | ISSN 1678-0817 | v. 30, n. 159, 2026 | DOI: 10.69849/shd64m04

Gerenciamento de riscos e controles internos no setor elétrico brasileiro: uma análise comparativa da AXIA, ENGIE e CPFL à luz do COSO ERM e da ISO 31000.

Risk management and internal controls in the brazilian electric power sector: a comparative analysis of AXIA, ENGIE, and CPFL in light of COSO ERM and ISO 31000.

Jhonatan da Costa Silveira[1]
Lorena Rocha Cavalcante[2]
Profa. Dra. Roberta Maia Said[3]

Resumo

O setor elétrico brasileiro está exposto a riscos regulatórios, operacionais, climáticos e tecnológicos, exigindo mecanismos eficazes de gerenciamento de riscos e controles internos. Nesse contexto, esta pesquisa teve como objetivo analisar o grau de aderência das práticas de gerenciamento de riscos e controles internos reportadas por Axia Energia, Engie Brasil e CPFL Energia às diretrizes dos frameworks COSO ERM (2017) e ISO 31000:2018. Trata-se de uma pesquisa descritiva, de abordagem qualitativa, desenvolvida por meio de pesquisa documental com base nos Formulários de Referência (FRE) divulgados pelas companhias à Comissão de Valores Mobiliários (CVM). A análise foi realizada por meio de uma matriz de confronto entre os principais fatores de risco, os mecanismos mitigadores declarados e os elementos previstos nos frameworks analisados, permitindo a classificação do grau de aderência das organizações. Os resultados evidenciaram convergência entre os riscos reportados pelas empresas, concentrados principalmente em aspectos regulatórios, climáticos, operacionais, tecnológicos e relacionados à continuidade das concessões. A Axia Energia apresentou aderência elevada à maioria dos elementos avaliados, destacando-se pelo alinhamento explícito ao COSO ERM (2017), à ISO 31000:2018 e à adoção do modelo das Três Linhas de Defesa. A CPFL Energia também demonstrou elevado grau de aderência, enquanto a Engie Brasil apresentou aderência predominantemente moderada. Conclui-se que as três companhias possuem estruturas formais de gerenciamento de riscos e controles internos, embora com diferentes níveis de aderência aos frameworks internacionais analisados.

Palavras-chave: gerenciamento de riscos; controles internos; COSO ERM; ISO 31000; setor elétrico.

[1] Pós-Graduando no MBA em Auditoria e Controladoria. Universidade do Estado do Amazonas (UEA).
[2] Pós-Graduando no MBA em Auditoria e Controladoria. Universidade do Estado do Amazonas (UEA).
[3] Professora no MBA em Auditoria e Controladoria. Universidade do Estado do Amazonas (UEA).

Abstract

The Brazilian electric power sector is exposed to regulatory, operational, climatic, and technological risks, requiring effective risk management and internal control mechanisms. This study aimed to analyze the degree of adherence of the risk management and internal control practices reported by Axia Energia, Engie Brasil, and CPFL Energia to the COSO ERM (2017) and ISO 31000:2018 frameworks. This is a descriptive study with a qualitative approach, based on documentary research using the Reference Forms disclosed by the companies to the Brazilian Securities and Exchange Commission (CVM). The analysis was conducted through a confrontation matrix between the main risk factors, the mitigation mechanisms reported, and the elements prescribed by the analyzed frameworks, allowing the classification of the organizations' degree of adherence. The results revealed convergence among the risks reported by the companies, mainly related to regulatory, climatic, operational, technological, and concession continuity issues. Axia Energia showed a high degree of adherence to most evaluated elements, standing out for its explicit alignment with COSO ERM (2017), ISO 31000:2018, and the Three Lines of Defense model. CPFL Energia also demonstrated a high degree of adherence, whereas Engie Brasil presented a predominantly moderate degree of adherence. It is concluded that the three companies have formal risk management and internal control structures, although with different levels of adherence to the international frameworks analyzed.

Keywords: risk management; internal controls; COSO ERM; ISO 31000; electric power sector.

1. INTRODUÇÃO

O setor elétrico brasileiro é complexo e passa por profundas mudanças estruturais, causadas pelas privatizações e pela divisão entre o mercado livre de geração e o mercado regulado de distribuição. As alterações frequentes nas regras criadas pela Agência Nacional de Energia Elétrica (ANEEL) e pelo Ministério de Minas e Energia (MME) exigem adaptação contínua das empresas (Tolmasquim, 2012). Somando-se a isso, há a grande dependência das usinas hidrelétricas do regime de chuvas em tempos de mudanças climáticas, gerando um elevado risco climático e hidrológico. Por isso, é essencial adotar uma postura de prevenção e monitoramento de longo prazo, superando ações voltadas apenas para o curto prazo (Kelman, 2009).Essa instabilidade regulatória e climática não repercute apenas na operação técnica das usinas, mas impacta diretamente a sustentabilidade financeira, a atratividade de investimentos e a transparência do mercado de capitais. Diante de um cenário onde a volatilidade dos preços e a escassez hídrica podem comprometer o valor de mercado das companhias, a capacidade de antever riscos deixa de ser uma vantagem competitiva e passa a ser uma condição de sobrevivência. Torna-se imperativo, portanto, compreender como essas organizações traduzem tais vulnerabilidades externas em seus mecanismos de defesa e prestação de contas.

Diante de tantas incertezas climáticas e regulatórias, as empresas precisam construir estruturas focadas em controle interno. Nesse sentido, a Governança Corporativa desempenha o papel fundamental de proteger os ativos e reduzir a assimetria de informação entre os departamentos e os investidores (Silveira, 2004). Mas, para esse sistema funcionar, os

controles internos devem ser preventivos e ativamente apoiados pela alta administração (*tone at the top*). Como apontam Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2017), "a administração e o conselho de administração estabelecem o tom no topo em relação à importância dos controles internos, incluindo as normas de conduta esperadas". No mesmo sentido, conforme Guerra (2021), o exemplo que vem da alta administração é o pilar fundamental para a disseminação de uma cultura de conformidade e ética por toda a empresa. Focado na conformidade e na mitigação de perdas, este artigo define seu problema de pesquisa: ***Qual é o grau de aderência às práticas de gerenciamento de riscos e controles internos das empresas do setor elétrico — declaradas nos Formulários de Referência da CVM — frente às diretrizes dos frameworks COSO ERM e ISO 31000?***

Assim, o Objetivo Geral da pesquisa é: analisar o grau de aderência das práticas de gerenciamento de riscos e controles internos da empresas Axia Energia, Engie Brasil e CPFL Energia — reportadas nos Formulários de Referência da CVM — em relação às diretrizes dos frameworks COSO ERM e ISO 31000.

Para atingir essa meta, os Objetivos Específicos buscam:

i. Mapear os cinco principais fatores de risco (Item 4 do FRE) identificados por cada companhia;
ii. Identificar os mecanismos de controle mitigadores (Item 5 do FRE) e sua relação com os riscos declarados; e,
iii. Descrever as limitações e as lacunas conceituais identificadas entre as diretrizes teóricas (COSO/ISO) e a prática de prevenção reportada pelas empresas.

A justificativa deste estudo baseia-se na oportunidade de comparar dados gerados após a Resolução CVM 80. Essa norma ampliou a *accountability* ao unificar, nos itens 4 e 5 do Formulário de Referência (FRE), as informações sobre fatores de risco e seus respectivos mecanismos de mitigação. A partir dessa nova base de transparência, torna-se relevante analisar como ocorre o redesenho de processos em uma corporação recém-privatizada, como a Axia Energia, comparando com empresas já consolidadas no mercado privado, como a Engie Brasil e a CPFL Energia.

Do ponto de vista acadêmico, esta pesquisa justifica-se ao preencher uma lacuna na literatura nacional sobre a eficácia empírica das estruturas de governança corporativa no setor regulado. Ao investigar os Formulários de Referência da CVM, o estudo avança no debate científico sobre a transparência informacional, analisando criticamente se o discurso corporativo reportado ao mercado reflete uma real aderência prática aos *frameworks* globais de risco (COSO ERM e ISO 31000) ou se configura apenas uma conformidade protocolar (*checklist*). Sob a ótica social, o estudo possui relevância pública incontestável, visto que o setor elétrico funciona como a infraestrutura de base para o desenvolvimento econômico do país. Falhas no gerenciamento de seus riscos regulatórios e climáticos ultrapassam as fronteiras corporativas: elas não apenas comprometem a saúde financeira e a continuidade operacional das companhias, mas deságuam em impactos socioeconômicos severos, que se traduzem na ameaça de desabastecimento, na instabilidade do fornecimento de energia para indústrias e hospitais, e no repasse inevitável de custos inflacionários diretamente às tarifas dos consumidores finais.

2. REFERENCIAL TEÓRICO

2.1. Setor Elétrico Brasileiro

2.1.1 Origem e Evolução do Modelo

O Brasil foi pioneiro no uso da eletricidade na América Latina, com registros que remetem ao final do século XIX, quando implementou suas primeiras instalações de iluminação pública permanente. Desde o início, o modelo do Setor Elétrico Brasileiro (SEB) desenvolveu características próprias que, mais tarde, serviram de referência para outros países.

O setor nasceu por meio da iniciativa privada. A empresa Light iniciou suas atividades em 1897, atuando no eixo Rio-São Paulo, enquanto a Amforp passou a adquirir concessionárias em outros centros urbanos a partir de 1927. Nessa época, os prazos dos contratos de concessão eram flexíveis e dependiam de acordos diretos com o poder concedente, variando entre 30 e 90 anos (Carneiro, 2003).

A estrutura moderna do SEB foi moldada pelas dimensões continentais do país e pelo seu vasto potencial hidrelétrico. Isso gerou um modelo centralizado, focado em grandes economias de escala e na cooperação entre empresas estatais. Esse sistema, consolidado com

a criação da Eletrobrás em 1963, utilizava o despacho centralizado de carga para otimizar o uso da água nas bacias hidrográficas, garantindo eficiência técnica e baixo custo operacional.

Contudo, esse modelo focado no Estado entrou em exaustão na década de 1980 devido a uma grave crise financeira e fiscal, marcada pelo alto endividamento das estatais e pelo uso das tarifas como ferramenta de controle da inflação. A transição para um modelo focado no mercado começou nos anos 1990, com o Plano Nacional de Desestatização, que buscava aumentar a produtividade, reduzir a dívida pública e atrair o capital privado para expandir a capacidade de geração do país.

2.1.2 Regulação: O Modelo Híbrido e a "Contra-Reforma"

Pouco tempo após as primeiras tentativas de privatização, o Brasil enfrentou uma crise de racionamento de energia em 2001, que gerou fortes impactos econômicos, sociais e políticos. Tolmasquim (2012) explica as causas daquele cenário:

> O racionamento foi um evento decorrente da vulnerabilidade presente no sistema elétrico desde 1999, causado primordialmente pelo atraso na entrada em operação de empreendimentos de geração e transmissão e pela ausência de novos projetos de geração para atender à demanda cujo crescimento ocorreu dentro do esperado no período.

Após o racionamento, o setor passou por uma reestruturação profunda em 2004, conhecida no meio acadêmico como "contra-reforma". A regulação evoluiu para acomodar a desverticalização do setor, separando as atividades de geração, transmissão, distribuição e comercialização. Para gerenciar esse novo ambiente, foram criados órgãos específicos: a ANEEL (regulação), o ONS (operação do sistema) e a CCEE (comercialização).

Esse modelo híbrido reintroduziu o planejamento estatal por meio da Empresa de Pesquisa Energética (EPE) e instituiu os leilões de energia para garantir a segurança do abastecimento. O mercado passou a ser dividido em dois ambientes: o **Ambiente de Contratação Regulada (ACR)** e o **Ambiente de Contratação Livre (ACL)**. Atualmente, a regulação brasileira ainda se baseia na formação de preços por custo, utilizando modelos computacionais que calculam o Custo Marginal de Operação (CMO) conforme o regime de chuvas.

2.1.3 Vulnerabilidades e a Proposta de Modernização

As vulnerabilidades atuais do setor estão na defasagem dos modelos de formação de preço e nos riscos ligados à abertura total do mercado. Rühle (2019) destaca que o sistema de

preços por custo já não reflete a realidade da operação real, tornando necessária a transição para modelos baseados em oferta, que ofereçam maior transparência e sinais econômicos corretos.

Entre as principais vulnerabilidades que exigem o desenho de processos preventivos nas empresas, destacam-se:

- **Poder de mercado e abusos:** no modelo de preço por oferta, há um risco elevado de manipulação de mercado por grandes agentes, principalmente em momentos de estresse do sistema ou de congestionamento nas redes de transmissão;
- **Vulnerabilidade financeira e judicialização:** intervenções regulatórias históricas causaram desequilíbrios profundos no mercado. Isso gerou uma judicialização em massa do risco hidrológico — conhecido como a disputa do *Generation Scaling Factor* (GSF) —, criando custos bilionários que acabam sendo repassados ao consumidor;
- **Complexidade na abertura do mercado:** a modernização do setor prevê a liberdade para que todos os consumidores acessem o mercado livre. No entanto, esse processo exige um arcabouço normativo rigoroso para evitar que a livre escolha resulte em falhas de suprimento ou abusos de poder econômico.

2.2 Governança Corporativa no Ambiente de Mercado de Capitais

No mercado de capitais, a governança corporativa serve para proteger os ativos e ajudar as empresas a enfrentarem incertezas. Segundo Silveira (2004), o papel principal da governança é reduzir conflitos de interesse: "Governança corporativa pode ser entendida como um conjunto de mecanismos de incentivo e controle, internos e externos, que visam a minimizar os custos decorrentes do problema de agência". Para que essa proteção funcione na prática e não seja apenas uma burocracia de fachada — o que Guerra (2021) chama de "governança do parecer ser" —, a estrutura da empresa precisa focar na "governança do ser". Isso significa aplicar de verdade os quatro pilares essenciais: transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa. É o desenho preventivo desses processos que garante um ambiente seguro e gera valor de longo prazo.

Esses pilares são fundamentais para reduzir a assimetria de informação, que ocorre quando a diretoria (os agentes) sabe muito mais sobre o dia a dia do negócio do que os investidores (os principais). Como os donos não controlam a empresa de perto, o risco de

perdas ou de decisões que favoreçam interesses particulares aumenta. Conforme alerta Guerra (2009), as grandes crises corporativas acontecem quando prevalecem "processos viciosos baseados em assimetria de informações, divergência de interesses e desacerto de propósitos". Por isso, ter um sistema de controle focado em prevenir problemas, e não apenas em reagir a eles, é a melhor defesa para alinhar as ações dos executivos aos objetivos dos acionistas.

Mas, para que a gestão de riscos saia do papel, essa cultura de conformidade precisa começar de cima — o chamado *Tone at the Top* (o tom do topo). O Conselho de Administração (CA) dita o ritmo da empresa e funciona como o guardião dessa mentalidade preventiva. De acordo com Guerra (2021), a responsabilidade de definir a conduta e os limites de riscos emana deste colegiado "é o CA que decide a estratégia da companhia, quais são os objetivos, o propósito e, mais importante, quais são os valores praticados."

Por fim, esse exemplo vindo do topo é vital para combater a centralização excessiva de poder. Guerra (2009) pontua que a realidade brasileira é diferente de outros mercados porque temos uma alta concentração acionária. Muitas vezes, o presidente do Conselho também é o acionista controlador ou alguém da família dele. Essa sobreposição de papéis concentra demais as decisões e enfraquece os controles criados para evitar abusos de poder. Portanto, um ambiente robusto exige descentralizar as aprovações e criar limites claros de alçadas, funcionando não como mera burocracia, mas como proteção real ao patrimônio da empresa.

2.3 A Norma ISO 31000 e as Diretrizes para a Gestão de Riscos

Para garantir o bom funcionamento do controle interno e do desenho de processos nas empresas, a ABNT NBR ISO 31000 é a principal referência técnica. A norma estabelece que para proteger os ativos e mitigar perdas, a gestão de riscos deve se basear em três princípios práticos: deve ser integrada (fazer parte de todas as atividades da empresa), estruturada e abrangente (para gerar resultados consistentes) e dinâmica (capaz de antecipar e responder rapidamente às mudanças nos contextos interno e externo) (ABNT, 2018).

Diferente da visão tradicional que associa o risco apenas a perdas, a norma traz uma abordagem mais ampla, definindo-o como o "efeito da incerteza nos objetivos" (ABNT, 2018). Essa definição mostra que a incerteza pode desviar a empresa do seu planejamento original, gerando impactos que "podem ser positivos, negativos ou ambos, criando

oportunidades e ameaças" (ABNT, 2018). Assim, a gestão de riscos deixa de ser reativa e passa a ser uma ferramenta contínua de adaptação estratégica.

Para manter esse dinamismo, a norma foca no desenho da estrutura (*framework design*). O objetivo é garantir que a gestão de riscos não seja uma burocracia isolada, mas "parte de todas as atividades da organização, incluindo a tomada de decisão" (ABNT, 2018). Esse desenho exige avaliar os ambientes interno e externo, garantir o compromisso da alta administração e mapear vulnerabilidades. Como o mercado muda rápido, o processo exige revisão constante. A norma determina que "o monitoramento contínuo e a análise crítica periódica [...] sejam uma parte planejada do processo [...], com responsabilidades claramente estabelecidas" (ABNT, 2018).

Esse modelo focado na prevenção atende diretamente à busca por conformidade e prestação de contas (*accountability*). A qualidade desse processo depende de controles que reduzam a assimetria de informação em cenários voláteis. Nesse sentido, Fontenelle e Silva (2015) destacam que o mercado exige cada vez mais transparência: "A qualidade e a fidedignidade das informações [...] são características que têm sido cada vez mais exigidas por seus usuários". Portanto, a ISO 31000, unida ao controle interno preventivo, reforça a visão dos autores de que fiscalizar os processos deve ser uma ação proativa, atuando como "uma importante técnica de controle [...] não só atuando para corrigir os desperdícios, a improbidade, a negligência e a omissão e, principalmente, antecipando-se a essas ocorrências" (Fontenelle e Silva, 2015). Essa estrutura garante que a gestão de riscos cumpra seu papel principal, que é proteger o patrimônio e dar sustentabilidade ao negócio no longo prazo.

2.4 O Framework COSO ERM (2017): Integração com Estratégia e Desempenho

As diretrizes do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) evoluíram para fortalecer o controle interno e a gestão preventiva nas empresas. Deixando para trás a visão antiga dos anos 1990 e de 2004, a versão atual do framework, chamada "Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance" (COSO, 2017), transformou a visão sobre o gerenciamento de riscos. O foco deixou de ser a mitigação de problemas em processos isolados e passou a ser a integração do gerenciamento de riscos com a estratégia do negócio. Assim, o controle preventivo deixa de ser uma peça estanque. Como aponta o manual do Ministério das Cidades (2024), a gestão de riscos não é uma função ou departamento. É a cultura, os recursos e as práticas que as organizações

integram com a estratégia definida e executada, com o objetivo de gerenciar o risco na criação, preservação e valorização".

Para colocar esse processo preventivo em prática, o COSO ERM (2017) se divide em cinco componentes inter-relacionados. A base de tudo está em Governança e Cultura, onde a governança dita o ritmo da empresa e define as responsabilidades de supervisão, enquanto a cultura alinha os valores éticos e os comportamentos de toda a equipe (COSO, 2017). Em seguida, o componente Estratégia e Definição de Objetivos garante que o apetite ao risco esteja alinhado ao planejamento estratégico. Dessa forma, as metas de negócios não apenas aplicam a estratégia, mas ajudam a identificar e responder aos riscos com antecedência (Arruda; Menchini; Russo, 2019). É nessa estrutura que as práticas de prevenção protegem os ativos de forma proativa.

O componente Informação, Comunicação e Reporte exige um fluxo contínuo de dados precisos em todos os níveis da empresa (COSO, 2017). Essa comunicação é decisiva, e é justamente nessa etapa de relatórios e consolidação de dados que empresas em transição, como a Axia Energia, costumam apresentar falhas graves. Lacunas de comunicação e a falta de um reporte fluido sobre os riscos enfraquecem as linhas de defesa e atrasam as respostas da alta administração. Sobre a necessidade de dados confiáveis para reduzir a assimetria de informações e garantir um controle preventivo robusto, Fontenelle e Silva (2015) advertem:

> A qualidade e a fidedignidade das informações, sejam elas referentes ao setor público ou privado, são características que têm sido cada vez mais exigidas por seus usuários. Isso se deve à facilidade e celeridade com que essas informações podem ser produzidas e divulgadas pelos meios de comunicação existentes.

Portanto, seguir à risca os componentes de comunicação e cultura desse framework garante que os controles internos funcionem de forma preventiva. A estrutura não serve apenas para conter danos, mas age antecipando-se a essas ocorrências (Fontenelle e Silva, 2015).

2.5 Sistemas de Controle Interno como Mecanismos Preventivos

Sob a ótica da Controladoria, as atividades de controle interno vão além da simples conferência do passado; elas são ferramentas essenciais para o funcionamento contínuo, eficiente e seguro das operações corporativas. O controle interno deve ser compreendido como um sistema integrado ao desenho de processos da empresa, criado para agir de forma proativa na mitigação de perdas e na garantia da conformidade (*compliance*). Ao analisar os

sistemas de informação gerencial, Padoveze (2010) aponta que a sustentabilidade de qualquer negócio depende de mecanismos próprios de monitoramento. O autor explica os componentes básicos que sustentam o controle de um sistema: [...] os controles e avaliações do sistema, para verificar a coerência entre os objetivos e as saídas [...]; a retroalimentação ou *feedback*, que pode ser considerado como reintrodução de uma saída sob a forma de informação, para proporcionar condições de autorregulamento. (Padoveze, 2010).

Nesse contexto, é preciso diferenciar os controles reativos dos controles preventivos. Os controles reativos operam na etapa do *feedback*, corrigindo erros ou mitigando danos somente após o problema ter acontecido. Embora ajudem a ajustar os rumos da empresa, eles são insuficientes em ambientes voláteis e complexos, como o setor elétrico brasileiro, pois não impedem o prejuízo financeiro inicial ou a exposição ao risco.

Em contrapartida, os controles preventivos são desenhados na origem da operação, evitando que o erro, a fraude ou a perda cheguem a acontecer. A eficácia da prevenção exige que a proteção esteja embutida na rotina da empresa desde o início. Corroborando essa lógica, Padoveze (2010) enfatiza que "a qualidade deve ser assegurada em todos os processos" e que "desde a ideia e desenvolvimento do produto é que os conceitos de custos e qualidade devem estar" presentes e operantes.

Na prática, esse desenho exige a implementação de mecanismos claros no dia a dia das companhias. Entre as principais atividades de controle preventivo essenciais para garantir a prestação de contas (*accountability*) e proteger os ativos, destacam-se:

- **Travas de sistemas:** parametrizações que barram automaticamente transações fora dos padrões preestabelecidos;
- **Segregação de funções:** divisão de tarefas desenhada para evitar a concentração de poder e inibir fraudes;
- **Alçadas de aprovação claras:** limites de gastos descentralizados e definidos com base na matriz de riscos;
- **Fluxos ágeis de comunicação:** conexão tempestiva entre o jurídico e o financeiro, garantindo que impactos contratuais e regulatórios sejam calculados antes de qualquer desembolso.

Ao integrar essas ferramentas no cotidiano da companhia, a Controladoria garante que o gerenciamento de riscos funcione como uma defesa proativa, e não como uma simples reação de curto prazo.

3. PROCEDIMENTOS METODOLÓGICOS

3.1 Classificação da Pesquisa

Nesta seção, definem-se os pilares científicos que sustentam a escolha metodológica da pesquisa:

- **Quanto à abordagem:** A pesquisa classifica-se como qualitativa, visto que a análise se concentra na interpretação crítica do texto dos relatórios corporativos das companhias, e não em mensurações ou métodos estatísticos.
- **Quanto aos objetivos:** Trata-se de uma pesquisa descritiva, pois o propósito é expor detalhadamente as características, as lacunas e a configuração atual dos controles preventivos declarados por essas empresas.
- **Quanto aos procedimentos:** Consiste em um estudo de caso múltiplo, uma vez que investiga e compara de forma independente as práticas de governança e a realidade de três organizações distintas (Axia, Engie e CPFL) operantes no mesmo setor elétrico brasileiro.

3.2 Coleta de Dados e Universo do Estudo

Esta etapa delimita o campo de observação e atesta a fidedignidade das fontes consultadas:

- **Universo da pesquisa:** O estudo delimita-se às empresas Axia Energia, Engie Brasil e CPFL Energia.
- **Fontes primárias:** Utilizam-se os Formulários de Referência (FRE) emitidos e atualizados pelas companhias no ano de 2026.
- **Recorte técnico:** O foco do download e da leitura restringe-se ao Item 4 (Fatores de Risco) e ao Item 5 (Gerenciamento de Riscos e Controles Internos) do FRE, cujas informações tiveram sua unificação e o detalhamento estabelecidos a partir da Resolução CVM 80.
- **Canal de coleta:** Os relatórios e documentos públicos foram obtidos de forma direta no sistema oficial e base de dados da Comissão de Valores Mobiliários (CVM).

3.3 Técnica de Análise dos Dados

A operacionalização para transformar a leitura dos relatórios (discurso corporativo) na matriz de achados práticos deu-se por meio da técnica de Confronto Matricial, dividida nos seguintes passos:

1. **Mapeamento:** Seleção e tabulação dos 5 principais fatores de risco reportados no Item 4 do FRE por cada uma das três empresas estudadas, cumprindo assim o objetivo específico 1 da pesquisa.
2. **Cruzamento:** Identificação manual (a partir do Item 5 do FRE) de qual atividade ou mecanismo de controle interno mitigador a companhia declarou possuir para enfrentar cada um dos riscos mapeados na etapa anterior, cumprindo o objetivo específico 2.
3. **Avaliação Teórica:** Análise qualitativa para descrever as limitações e avaliar o grau de aderência prática dos mecanismos reportados pelas empresas frente às diretrizes dos pilares preventivos do *framework* COSO ERM (2017) e da norma ISO 31000, cumprindo assim o objetivo específico 3.

Para avaliar o grau de aderência das práticas de gerenciamento de riscos e controles internos reportadas pelas empresas aos frameworks COSO ERM (2017) e ISO 31000:2018, foi elaborada uma matriz de análise composta por elementos considerados essenciais na literatura especializada, tais como existência de comitê de riscos, utilização do modelo de três linhas de defesa, monitoramento contínuo dos riscos, comunicação de riscos e realização de avaliações periódicas dos controles internos.

A análise foi realizada por meio da técnica de confronto matricial entre as informações constantes nos Formulários de Referência (FRE) e os requisitos conceituais previstos nos frameworks estudados. Neste sentido, a técnica de confronto matricial foi aplicada em duas etapas complementares. Na primeira etapa, os fatores de risco identificados nos Formulários de Referência foram confrontados com os respectivos mecanismos mitigadores declarados pelas companhias. Já na segunda etapa, os mecanismos de controle identificados foram confrontados com os elementos previstos nos frameworks COSO ERM (2017) e ISO 31000:2018, permitindo a classificação do grau de aderência das práticas reportadas.

Para cada elemento analisado, foi atribuído um grau de aderência, classificado em quatro níveis: (i) Aderência Elevada, quando a prática é claramente descrita e demonstra

alinhamento consistente com as diretrizes do COSO ERM ou da ISO 31000; (ii) Aderência Moderada, quando a prática é mencionada, porém com detalhamento limitado ou evidências parciais de implementação; (iii) Aderência Baixa, quando existem apenas indícios indiretos da prática, sem evidências suficientes para confirmar sua efetiva aplicação; e (iv) Aderência Ausente, quando não foram identificadas evidências da prática nos documentos analisados, conforme descritos no quadro 1.

Essa classificação permitiu comparar o nível de alinhamento das companhias estudadas em relação aos principais mecanismos de governança, gerenciamento de riscos e controles internos recomendados pelos frameworks internacionais.

Quadro 1: Elementos de análise e critérios para classificação do grau de aderência

Elemento Avaliado	**Critério de Verificação**	**Grau de Aderência**
Comitê de riscos	**Existência formal de comitê ou**	**Elevada / Moderada / Baixa /**
	estrutura equivalente	**Ausente**
Três linhas de defesa	**Menção explícita ao modelo ou estrutura equivalente**	**Elevada / Moderada / Baixa / Ausente**
Comunicação de riscos	**Fluxo formal de reporte de riscos**	**Elevada / Moderada / Baixa / Ausente**
Monitoramento contínuo	**Acompanhamento permanente dos riscos e controles**	**Elevada / Moderada / Baixa / Ausente**
Avaliação periódica	**Revisões ou testes periódicos dos controles internos**	**Elevada / Moderada / Baixa / Ausente**

Fonte: Elaboração própria.

4. ANÁLISES E DISCUSSÕES DOS RESULTADOS

Após análise dos resultados obtidos, o Quadro 2 apresenta o primeiro nível do confronto matricial, relacionando os fatores de risco aos mecanismos mitigadores declarados pelas companhias. Em seguida, o Quadro 3 apresenta o segundo nível do confronto matricial, no qual os mecanismos identificados foram avaliados à luz dos elementos previstos nos frameworks COSO ERM (2017) e ISO 31000:2018.

Para avaliar a maturidade da governança e dos controles preventivos no setor elétrico, os dados coletados nos Formulários de Referência (FRE) de 2026 foram consolidados em uma matriz de confronto. O Quadro 2 apresenta os cinco principais fatores de risco declarados por Axia, Engie e CPFL, acompanhados de suas respectivas ferramentas de controle e menções aos *frameworks* globais.

Quadro 2 – Matriz de Confronto entre Fatores de Risco e Mecanismos Mitigadores Declarados pelas Companhias

Empresa	Categoria de Risco	Principal risco reportado	Mecanismos mitigadores declarados	Evidências de governança e controle
Axia Energia	Concessões	Renovação de concessões e autorizações	Política de Gestão de Riscos e Controles Internos; planos de mitigação e conciliação	Conselho de Administração; Comitê de Auditoria e Riscos; Diretoria de Riscos, Conformidade e Controles
	Regulatório	Alterações regulatórias e legislativas	Política de riscos; alinhamento à ISO 31000 e COSO ERM	Estrutura formal de governança e reporte
	Climático / Hidrológico	Dependência de condições naturais para geração de energia	Identificação, avaliação e tratamento de riscos	Política de Gestão de Riscos e Controles Internos
	Tecnológico	Cibersegurança e dependência de sistemas digitais	Controles internos e monitoramento tecnológico	Três Linhas de Defesa

	Fornecedores / Terceiros	Dependência da cadeia de suprimentos e prestadores técnicos	Gestão de fornecedores e planos de mitigação	Monitoramento por áreas de risco, conformidade e controles
Engie Brasil	Licenciamento	Licenças, autorizações e concessões	Política de Gestão de Riscos e Oportunidades Empresariais	ERM e Comitê de Auditoria
	Regulatório	Mudanças nas normas do setor elétrico	Matriz de riscos; limites quantificáveis; políticas específicas	Estrutura funcional de gestão de riscos empresariais
	Climático	Mudanças climáticas e eventos extremos	Matriz de impacto e probabilidade	Certificações ISO 9001 e ISO 14001
	Operacional	Infraestrutura, construção e expansão de projetos	Políticas de gestão operacional e de investimentos	Auditoria Interna e Comitê de Auditoria
	Tecnológico	Sistemas digitais e segurança da informação	Gestão de riscos tecnológicos	Estrutura ERM e auditoria
CPFL Energia	Regulatório / Tarifário	Regulação tarifária definida pela ANEEL	Política de Gestão Corporativa de Riscos	Conselho de Administração e Comitê de Gestão de Riscos
	Concessões	Cumprimento e renovação de	Mapa Corporativo de Riscos	Monitoramento de limites de exposição
		concessões e autorizações		
	Fornecedores / Terceiros	Dependência de fornecedores e prestadores técnicos	Mapa de riscos e controles operacionais	Comitê de Gestão de Riscos
	Tecnológico	Segurança cibernética e proteção de dados	Controles de TI; programa de compliance; canal de ética	Auditoria Interna como terceira linha de defesa

	Climático	Condições climáticas e dependência de recursos naturais	Avaliação dos impactos climáticos e operacionais	Avaliação anual dos controles internos com base no COSO

Fonte: Elaborado pelos autores com base nos Formulários de Referência (2026).

Os resultados apresentados no Quadro 2 evidenciam elevada convergência entre os fatores de risco reportados pelas companhias analisadas. Em linhas gerais, os riscos identificados concentram-se em cinco grandes dimensões: regulatória, climática, operacional, tecnológica e relacionada à continuidade das concessões. Tal convergência reforça a literatura sobre o setor elétrico brasileiro, que aponta a forte dependência das empresas em relação à estabilidade regulatória, à disponibilidade de recursos naturais e à continuidade dos serviços públicos concedidos.

Observa-se também que, embora as organizações adotem mecanismos mitigadores semelhantes, como auditoria interna, políticas corporativas de gestão de riscos, comitês de supervisão e programas de *compliance*, existem diferenças relevantes quanto ao grau de formalização e ao alinhamento explícito dessas práticas aos *frameworks* internacionais de gerenciamento de riscos. Dessa forma, o confronto entre os riscos reportados e os mecanismos mitigadores declarados constitui a primeira etapa da análise matricial proposta neste estudo, servindo de base para a avaliação do grau de aderência das companhias aos elementos preconizados pelo COSO ERM (2017) e pela ISO 31000:2018, conforme apresentado no Quadro 3.

Quadro 3 – Avaliação do Grau de Aderência aos Frameworks COSO ERM (2017) e ISO 31000:2018

Elemento Avaliado	Axia	Engie	CPFL
Comitê de Riscos	Elevada	Moderada	Elevada
Três Linhas de Defesa	Elevada	Ausente	Moderada
Comunicação de Riscos	Moderada	Moderada	Elevada
Monitoramento Contínuo	Elevada	Elevada	Elevada
Avaliação Periódica dos Controles	Elevada	Moderada	Elevada

Fonte: Elaboração própria com base nos Formulários de Referência (2026).

Com base na matriz de aderência elaborada para esta pesquisa, observa-se que as três companhias apresentam evidências de adoção de mecanismos formais de gerenciamento de riscos e controles internos. Entretanto, o grau de aderência aos elementos analisados não se apresenta de forma homogênea entre as organizações.

A Axia Energia destacou-se por apresentar evidências consistentes de alinhamento às diretrizes do COSO ERM (2017) e da ISO 31000:2018, sendo a única companhia a declarar explicitamente a utilização simultânea desses frameworks, além da adoção formal da metodologia das Três Linhas de Defesa. Tais características contribuíram para a classificação de aderência elevada em grande parte dos elementos avaliados.

Já a CPFL Energia também apresentou elevado grau de aderência, especialmente em aspectos relacionados ao monitoramento contínuo dos riscos, à avaliação periódica dos controles internos e à existência de estruturas formais de governança, como o Comitê de Gestão de Riscos. Adicionalmente, a certificação ISO 37001 associada ao Programa de Integridade reforça o compromisso da companhia com práticas de *compliance* e controles corporativos.

Por sua vez, a Engie Brasil demonstrou aderência predominantemente moderada. Embora a empresa apresente mecanismos estruturados de gestão de riscos, auditoria interna, comitê de auditoria e matriz de riscos corporativos, não foram identificadas evidências suficientes para confirmar aderência elevada em alguns dos elementos analisados, especialmente quanto à adoção formal do modelo das Três Linhas de Defesa e à existência de mecanismos explicitamente reportados de avaliação periódica dos controles internos. Dessa forma, os resultados sugerem que a companhia possui uma estrutura consistente de gerenciamento de riscos, ainda que com menor grau de formalização em relação aos elementos avaliados nesta pesquisa, conforme sintetizado no Quadro 3.

A partir do mapeamento apresentado acima, a análise crítica dos resultados fundamenta-se em três blocos de discussão:

1. A Convergência dos Riscos no Setor Elétrico

Os riscos reportados pelas três companhias apresentam elevada convergência, concentrando-se principalmente em cinco dimensões: regulatória, climática, operacional, tecnológica e relacionada à continuidade das concessões. Esse cenário reforça os argumentos

apresentados por Tolmasquim (2012), Kelman (2009) e Soares (2024), segundo os quais o setor elétrico brasileiro está naturalmente exposto a fatores externos capazes de impactar significativamente a continuidade dos negócios.

A forte dependência dos recursos hídricos, associada aos efeitos das mudanças climáticas, amplia a exposição ao risco hidrológico, enquanto alterações regulatórias promovidas por órgãos como a ANEEL e o Ministério de Minas e Energia podem afetar diretamente a rentabilidade e a sustentabilidade econômico-financeira das concessões. Nesse contexto, a capacidade de identificar, monitorar e mitigar riscos deixa de representar apenas uma vantagem competitiva e passa a constituir requisito essencial para a continuidade operacional das organizações.

2. Evidências de aderência formal aos frameworks internacionais

Um dos principais achados da pesquisa refere-se à posição da Axia Energia em relação aos elementos avaliados na matriz de aderência. Entre as companhias analisadas, a Axia foi a única a declarar explicitamente alinhamento simultâneo ao COSO ERM (2017) e à ISO 31000:2018, além de mencionar formalmente a utilização do modelo das Três Linhas de Defesa. Tais evidências contribuíram para sua classificação com aderência elevada em grande parte dos elementos analisados. Sob a perspectiva de Guerra (2021), esse resultado sugere uma estrutura formal de governança e gerenciamento de riscos alinhada às boas práticas internacionais. Entretanto, considerando que a análise se restringiu aos Formulários de Referência, não é possível afirmar se a aderência formal observada se traduz integralmente em efetividade prática na gestão cotidiana dos riscos organizacionais.

3. Engie (Foco Operacional) vs. CPFL (Foco em Compliance)

Também há uma diferença clara entre a Engie e a CPFL, que usam caminhos diferentes para controlar seus riscos. A Engie foca em uma governança muito prática e

operacional, usando matrizes de probabilidade, gestão de oportunidades e selos de qualidade e meio ambiente (ISO 9001 e ISO 14001). Já a CPFL demonstra uma preocupação

muito maior com a conformidade (*compliance*) e com as regras de tarifas. Isso fica claro porque ela segue os padrões do COSO 2013 e é a única que buscou a certificação ISO 37001 (Antissuborno) para o seu Programa de Integridade.

Sob a perspectiva de Padoveze (2010), observa-se que ambas as companhias adotam mecanismos voltados ao monitoramento e ao controle dos riscos organizacionais, ainda que com enfoques distintos. Enquanto a Engie privilegia instrumentos relacionados à gestão operacional e à avaliação sistemática dos riscos, a CPFL demonstra maior ênfase em estruturas formais de compliance, integridade e supervisão. Em ambos os casos, os mecanismos identificados contribuem para reduzir a assimetria de informações, fortalecer os processos de governança e ampliar a capacidade organizacional de resposta às incertezas inerentes ao setor elétrico.

5. CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo analisar o grau de aderência das práticas de gerenciamento de riscos e controles internos reportadas por Axia Energia, Engie Brasil e CPFL Energia nos Formulários de Referência da CVM, em relação às diretrizes dos frameworks COSO ERM (2017) e ISO 31000:2018. Para tanto, buscou-se responder à seguinte questão de pesquisa: qual é o grau de aderência das práticas de gerenciamento de riscos e controles internos declaradas pelas empresas do setor elétrico frente às diretrizes desses frameworks internacionais?

Os resultados evidenciaram que as três companhias reconhecem e reportam riscos semelhantes, concentrados principalmente em aspectos regulatórios, climáticos, operacionais, tecnológicos e relacionados à continuidade das concessões. Tal convergência confirma a literatura sobre o setor elétrico brasileiro, especialmente os estudos de Tolmasquim (2012), Kelman (2009) e Soares (2024), que destacam a elevada exposição das empresas do segmento a mudanças regulatórias e à dependência de fatores hidrológicos e climáticos.

No que se refere aos mecanismos mitigadores, observou-se que as empresas utilizam diferentes estruturas de governança, gerenciamento de riscos e controles internos para responder às vulnerabilidades identificadas. A Axia Energia apresentou aderência elevada na maioria dos elementos, sendo a única companhia a declarar explicitamente alinhamento

simultâneo ao COSO ERM (2017) e à ISO 31000:2018, além da adoção do modelo das Três Linhas de Defesa. A CPFL Energia também apresentou elevado grau de aderência, destacando-se pela existência de estruturas formais de monitoramento de riscos, auditoria interna e certificação ISO 37001 vinculada ao seu programa de integridade.

Já a Engie Brasil demonstrou aderência predominantemente moderada, uma vez que, embora apresente mecanismos estruturados de gestão de riscos, auditoria interna e monitoramento corporativo, não foram identificadas evidências suficientes para confirmar aderência elevada em alguns dos elementos avaliados, especialmente quanto à adoção formal do modelo das Três Linhas de Defesa e à avaliação periódica dos controles internos.

Os achados corroboram os pressupostos teóricos apresentados por COSO (2017) e ABNT (2018), ao demonstrarem que a efetividade da gestão de riscos depende da integração entre governança, comunicação, monitoramento e definição clara de responsabilidades. Da mesma forma, os resultados reforçam as reflexões de Guerra (2021) acerca da necessidade de que as estruturas formais de governança sejam efetivamente incorporadas à cultura organizacional, superando uma lógica meramente formal de conformidade. Os resultados também convergem com Padoveze (2010), ao evidenciar a importância dos mecanismos de monitoramento, feedback e controle como instrumentos de proteção patrimonial e suporte à tomada de decisão.

Embora os resultados indiquem diferentes níveis de aderência formal aos *frameworks* analisados, a pesquisa não permite concluir sobre a efetividade prática desses mecanismos no cotidiano das organizações, uma vez que a análise foi realizada exclusivamente com base nas informações divulgadas nos Formulários de Referência da CVM. Assim, os resultados refletem as práticas reportadas pelas companhias ao mercado, não sendo possível verificar empiricamente a implementação ou o desempenho efetivo dos controles internos descritos.

Como limitação metodológica, destaca-se a utilização exclusiva de dados documentais provenientes dos Formulários de Referência, bem como a restrição da amostra a três companhias do setor elétrico brasileiro. Dessa forma, os resultados não podem ser generalizados para todas as empresas do setor ou para outros segmentos econômicos.

Por fim, recomenda-se que pesquisas futuras ampliem a amostra analisada, incluam outros setores regulados e adotem métodos complementares, como entrevistas com gestores, membros de comitês de auditoria e responsáveis pela gestão de riscos. Estudos de caso aprofundados também poderão contribuir para avaliar não apenas a aderência formal aos

frameworks COSO ERM e ISO 31000, mas principalmente a efetividade prática dos mecanismos de governança, gerenciamento de riscos e controles internos implementados pelas organizações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: Gestão de riscos — Diretrizes. 2. ed. Rio de Janeiro: ABNT, 2018.

ARRUDA, C. L.; MENCHINI, F.; RUSSO, P. T. Percepção sobre os fatores do gerenciamento de riscos corporativos que influenciam o planejamento estratégico. **Future Studies Research Journal: Trends and Strategies**, [S.l.], 2019.

BERNARDINO, F. F. M.; PEIXOTO, F. M.; FERREIRA, R. do N. Governança e eficiência em empresas do setor elétrico brasileiro. **Revista Pretexto**, Belo Horizonte, 2015.

BRASIL. Ministério das Cidades. Assessoria Especial de Controle Interno. **Metodologia de gestão de riscos estratégicos**. Brasília: Ministério das Cidades, Governo Federal, 2024.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Performance**: Sumário Executivo. [S.l.]: COSO; PwC, 2017.

FERREIRA, C. K. L. Privatização do setor elétrico no Brasil. [S.l.]: [s.n.], [199-].

FONTENELLE, R; SILVA, C. A. T. Limites da auditoria financeira no setor público. In: CONGRESSO USP DE CONTROLADORIA E CONTABILIDADE, 15., 2015, São Paulo. **Anais** [...]. São Paulo: FEA-USP, 2015.

GUERRA, S. **A caixa-preta da governança**. 4. ed. [S.l.]: [s.n.], [s.d.].

GUERRA, S. **Os papéis do conselho de administração em empresas listadas no Brasil**. 2009. 214 f. Dissertação (Mestrado em Administração) – Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2009.

KELMAN, R. **Planejamento coordenado dos setores de energia elétrica e gás natural**. 2009. 181 f. Tese (Doutorado em Engenharia de Sistemas e Computação) – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (COPPE), Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2009.

PADOVEZE, C. L. **Contabilidade gerencial**: um enfoque em sistema de informação contábil. 7. ed. São Paulo: Atlas, 2010.

RÜHLE, B. B. **A modernização do setor elétrico brasileiro e a sua regulação para prevenir abusos de mercado**. 2019. 69 f. Monografia (Bacharelado em Direito) – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2019.

SILVEIRA, A. D. M. da. **Governança corporativa e estrutura de propriedade**: determinantes e relação com o desempenho das empresas no Brasil. 2004. 250 f. Tese (Doutorado em Administração) – Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2004.

SILVEIRA, A. D. M. da; BARROS, L. A. B. de C. Determinantes da qualidade da governança corporativa das companhias abertas brasileiras. **REAd – Revista Eletrônica de Administração**, Porto Alegre, v. 14, n. 3, set./dez. 2008.

SOARES, M. de A. **Análise regulatória das crises hídricas enfrentadas em 2001 e 2021 no setor elétrico brasileiro**. 2024. 104 f. Dissertação (Mestrado em Ciências da Energia) – Instituto de Energia e Ambiente, Universidade de São Paulo, São Paulo, 2024.

TOLMASQUIM, M. T. Perspectivas e planejamento do setor energético no Brasil. **Estudos Avançados**, São Paulo, v. 26, n. 74, p. 247-260, 2012.

TOLMASQUIM, M. T.; GUERREIRO, A.; GORINI, R. Matriz energética brasileira. **Novos Estudos CEBRAP**, São Paulo, n. 79, p. 47-69, nov. 2007.