Política de Gestão Estratégica de Riscos e Controles Internos

CELESC

Política de Gestão Estratégica de Riscos e Controles Internos

SUMÁRIO

1. INTRODUÇÃO

Fica estabelecida para as Centrais Elétricas de Santa Catarina S.A. (Celesc S.A.) e suas subsidiárias integrais, dirigentes, empregados, fornecedores, prestadores de serviço e parceiros de negócio, bem como todos os profissionais que atuem em seu nome, a Política de Gestão Estratégica de Riscos e Controles Internos, que define objetivos, conceitos, princípios, diretrizes e responsabilidades, com a finalidade de estruturar um sistema de gestão de riscos e controles internos, de forma a fortalecer a governança e contribuir com o alcance dos objetivos estratégicos da organização, aplicável aos Riscos Corporativos, Riscos de Reporte Financeiro e Riscos de Integridade.

2. OBJETIVOS

- Contribuir para o alcance dos objetivos do Plano Diretor da organização, através de mecanismos de mitigação dos riscos;
- Incentivar as boas práticas de Governança Corporativa;
- Melhorar o desempenho organizacional;
- Reduzir o impacto de perdas advindas das incertezas do mercado;
- Proporcionar melhores oportunidades de geração de valor para a organização;
- Contribuir para a tomada de decisões;
- Contribuir com a efetividade do Programa de Compliance.

3. CONCEITOS

- Ambiente Corporativo - Também conhecido por *Entity Level Control* – ELC, é a avaliação dos controles no nível da entidade, não estando necessariamente endereçados a processos específicos, pois permeiam toda a organização.

- Ambiente de Negócios - Também conhecido por *Process Level Control* – PLC, é a avaliação dos controles internos no nível de processo e são desempenhados de forma específica vinculada diretamente às operações e aos processos da empresa.

- Ambiente Tecnológico - Também conhecido por Controles Gerais de Tecnologia da Informação/*IT General Controls* – ITGC, é a avaliação dos controles em nível de sistemas que proporcionam suporte aos macroprocessos selecionados pela materialidade das demonstrações financeiras.

- Apetite ao Risco - Representa o quanto a empresa está disposta a se expor frente aos seus riscos.

- Controle Efetivo - É o resultado de teste que identifica que os controles operam adequadamente de forma a mitigar o risco de reporte financeiro.

- Controle Não Efetivo - É o resultado de teste que identifica deficiências de controle ou exceções à efetividade dos controles.

- Controles Internos - Processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

- Criticidade do Risco - Nível de Exposição de um risco conforme sua probabilidade e impacto.

- Fatores de Risco - São ocorrências específicas que, por si só ou combinadas com outras, podem gerar um risco para a organização.

- Gestão de Riscos Corporativos - Princípios, cultura, competências e práticas que a organização integra à definição e à execução da estratégia, com o objetivo de gerenciar os riscos na criação, preservação e realização de valor.

- Governança Corporativa - Sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo o relacionamento entre Conselho, equipe executiva e demais órgãos de controle. As boas práticas de governança convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar a reputação da organização e de otimizar seu valor social, facilitando seu acesso a recursos e contribuindo para sua longevidade.

- Mapa de Riscos Corporativos - Mapa contendo o posicionamento dos Riscos Corporativos de acordo com seu impacto e probabilidade de ocorrência.

- Mapeamento de Processos - Atividade na qual todos os processos de uma determinada área são identificados, classificados e segmentados, definindo periodicidade, responsáveis, fluxo de informações, atividades encadeadas e relacionamento entre áreas.

- Materialidade - É o planejamento estratégico para o mapeamento de Controles Internos, por meio de critérios quantitativos e qualitativos, com o objetivo de identificar os processos que estão relacionados às contas de maior representatividade nas Demonstrações Financeiras.

- Programa de Compliance - Conjunto de instrumentos e procedimentos voltados para garantir a conduta ética no ambiente da Celesc, tendo como guia o rol de legislações aplicáveis e o conjunto de regras internas sobre conduta ética. O Programa visa atuar na prevenção, detecção, resposta e correção de possíveis atos de fraude, corrupção e desvios de conduta ética.

- Recomendações - Iniciativas ou planos de ação com objetivo de implementar controles aos processos ou melhorias nos controles existentes.

- Risco de Integridade - São os riscos de vulnerabilidade institucional que podem favorecer ou facilitar práticas de corrupção, fraudes, subornos, irregularidades e desvios éticos e de conduta.

- Risco de Reporte Financeiro - É o risco de omissão ou distorção nas Demonstrações Financeiras em razão de erro ou fraude. É específico para a divulgação das Demonstrações Financeiras, voltado para a representação fidedigna das informações.

- Riscos - São eventos incertos que podem gerar impactos negativos, positivos ou ambos.

- Sistema de Gestão Estratégica de Riscos e Controles Internos - Conjunto de componentes responsáveis pela implantação e melhoria contínua da Gestão Estratégica de Riscos e Controles Internos da Organização.

- Testes de Desenho ou *Test of Design* (TOD) - É a validação do desenho do controle, ou seja, é a comprovação da existência dos controles para mitigar os riscos de reporte financeiro identificados no mapeamento ou após a implementação.

- Testes de Efetividade ou *Test of Effectiveness* (TOE) - É a comprovação de que o controle opera adequada e oportunamente, possibilitando a mitigação do risco de reporte financeiro identificado.

- Três linhas de gerenciamento de riscos - Modelo que ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma

forte governança e gerenciamento de riscos.

4. PRINCÍPIOS

A Política de Gestão Estratégica de Riscos e Controles Internos da Celesc S.A. e suas Subsidiárias integrais, visando contribuir para o alcance dos objetivos estratégicos da organização, está orientada pelos seguintes princípios:

- Estar alinhada com o Plano Diretor e com as estratégias organizacionais *(COSO);*
- Agregar e proteger valor *(COSO/ISO)*;
- Integrar todas as atividades organizacionais *(ISO)*;
- Abordar explicitamente a incerteza e se antecipar às mudanças *(COSO);*
- Melhorar a performance da organização *(COSO)*;
- Estar alinhada com o contexto interno e externo da organização;
- Considerar fatores humanos e culturais *(ISO)*;
- Ser transparente, inclusiva, estruturada e abrangente *(ISO);*
- Ser dinâmica, interativa e capaz de reagir a mudanças *(ISO)*;
- Facilitar a melhoria contínua da organização *(ISO)*;
- Utilizar padrões e metodologias reconhecidas;
- Alertar a organização para seus riscos de negócio e processos de forma independente e neutra;

- Melhorar e alavancar sistemas de informação, comunicação e divulgação *(ISO/COSO);*

- Atuar em consonância com os princípios e valores dispostos no Código de Conduta Ética da Celesc.

5. DIRETRIZES

Para assegurar que a Gestão Estratégica de Riscos e Controles Internos da Celesc sejam executados de forma a prevenir ou mitigar os riscos, as seguintes diretrizes deverão ser observadas:

- Informar e comunicar continuamente todos os níveis da organização a respeito da importância e dos resultados dos processos de Gestão de Riscos e Controles Internos;
- Disponibilizar as informações de interesse das partes interessadas com transparência;
- Capacitar, treinar e conscientizar os empregados para geração de bases fundamentais de Gestão de Riscos e Controles Internos;
- Integrar sistematicamente o processo de Gestão de Riscos e Controles Internos, buscando o envolvimento de todos os responsáveis;
- Definir responsabilidades, delegação de poderes e segregação de funções dos empregados na Gestão de Riscos e Controles Internos;
- Acompanhar e avaliar a exposição definida pelos gestores frente aos seus riscos estratégicos;
- Estabelecer controles internos de acordo com os procedimentos da empresa de forma a prevenir e mitigar os riscos;
- Analisar as decisões a serem tomadas procurando levar em consideração os riscos previamente identificados;
- Disponibilizar infraestrutura e recursos necessários para a adequada execução;
- Garantir o funcionamento das três linhas de gerenciamento de riscos.

6. PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS

O Processo de Gestão de Riscos Corporativos compreende o conjunto de recursos e atividades que envolvem a análise do contexto organizacional, identificação, análise, avaliação e tratamento dos riscos corporativos, bem como o monitoramento e comunicação dessas atividades.

O processo de Gestão de Riscos Corporativos se desenvolve através das seguintes atividades:

Comunicação e Consulta

A comunicação busca informar e conscientizar sobre o entendimento dos riscos, durante todas as fases da Gestão de Riscos Corporativos, além de consultar informações para auxiliar a tomada de decisão. Deve abordar questões relacionadas com o risco, suas causas (fatores de riscos), suas consequências e as medidas que estão sendo tomadas para tratá-los.

Definição de Escopo, Contexto e Critérios

Tem por objetivo alinhar os riscos aos objetivos estratégicos e à estratégia da Celesc, considerando os ambientes interno e externo da companhia, além de definir critérios para a análise do risco e limites de tolerância.

Avaliação de Riscos

Compreende a identificação, análise e avaliação de riscos, envolvendo as partes interessadas e utilizando a melhor informação disponível.

a) **Identificação dos Riscos** – Levantamento dos riscos e seus fatores de risco que possam interferir no alcance dos objetivos estratégicos da Celesc e irão compor a Árvore de Riscos, aprovada pela Alta Administração.

b) **Análise dos Riscos** – Compreensão da natureza do risco, características, e o seu nível. Deve-se considerar as incertezas, fontes de risco, consequências, probabilidade, impacto, cenários, processos críticos, controles e sua eficácia. A análise pode ser quantitativa, qualitativa ou pela combinação de ambas. Com a avaliação de probabilidade e impacto, é gerada a matriz de riscos corporativos da Celesc, que evidencia a criticidade dos riscos.

c) **Avaliação dos Riscos** – Avalia a necessidade de tratamento dos riscos analisados, qual a estratégia e métodos mais apropriados. Envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos e servem para determinar onde é necessária ação adicional.

Tratamento dos Riscos

Envolve selecionar a opção mais adequada, considerando o seu custo-benefício em relação ao alcance dos objetivos da organização, considerando critérios de risco estabelecidos e recursos disponíveis. A Diretoria Executiva é responsável pelo endereçamento de planos de ação e controles internos para mitigação dos riscos identificados. A Diretoria executiva pode decidir ainda por assumir, evitar ou compartilhar um risco, conforme estabelecido na ISO 31000:2018.

Monitoramento e Análise Crítica

Consiste em verificar a eficiência e eficácia do processo e implementar as melhorias necessárias. Monitorar o desempenho dos indicadores, planos de ação e as mudanças no cenário do risco. Tratamentos não eficazes devem manter a análise crítica contínua sobre o risco. O risco remanescente deve ser registrado e submetido a monitoramento, análise crítica e, quando apropriado, tratamento adicional.

Registro e Relato

O processo de gestão de riscos deve ser documentado, relatar as atividades e resultados da gestão de riscos e fornecer informações para a tomada de decisão.

7. PROCESSO DE GESTÃO DE RISCOS DE REPORTE FINANCEIRO

O Processo de Gestão dos Riscos de Reporte Financeiro pode interagir com todas as áreas da organização e seus ambientes de avaliação podem ser segregados em três níveis: Ambiente Corporativo ou Controles no Nível de Entidade, Ambiente de Negócios ou Controles no Nível de Processo e Ambiente Tecnológico ou Controles Gerais de Tecnologia da Informação.

O processo de avaliação dos controles internos para a gestão dos riscos de reporte financeiro tem como objetivo a transparência e veracidade sobre a elaboração e divulgação das Demonstrações Financeiras e obedecerá, em linhas gerais, às seguintes fases:

Análise da Materialidade

Realização do cálculo de materialidade, para definição do escopo dos trabalhos.

Entendimento dos Processos

Entendimento dos processos por meio de entrevistas com as áreas e elaboração de narrativas e/ou mapeamento das atividades.

Elaboração da Matriz de Riscos e Controles

Elaboração da Matriz de Riscos de Reporte Financeiro com identificação e registro dos riscos e controles do processo.

Realização dos Testes de Desenho dos controles

Avaliação da efetividade do desenho dos controles.

Recomendações

Elaboração das recomendações de melhorias ou implementação de novos controles.

Acompanhamento dos Planos de Ação

Monitoramento contínuo dos Planos de Ação das Melhorias ou de Implementação de Novos Controles.

Realização dos Testes de Efetividade

Avaliação da efetividade dos controles.

Consolidação dos Resultados

Elaboração de relatório e validação com os responsáveis.

Reportes dos Resultados dos Testes de Efetividade

Reporte às áreas responsáveis pelos riscos e controles, reporte à Diretoria Executiva e reporte ao Conselho de Administração por meio do Comitê de Auditoria Estatutário – CAE.

8. PROCESSO DE GESTÃO DE RISCOS DE INTEGRIDADE

O Processo de Gestão de Riscos de Integridade, vinculado ao Programa de Compliance, busca identificar, analisar, avaliar, tratar, monitorar e reportar os riscos de integridade.

Consideram-se riscos de integridade aqueles que representam vulnerabilidade institucional que podem favorecer ou facilitar práticas de corrupção, fraudes, subornos, irregularidades e desvios éticos e de conduta.

Nesse escopo, o Processo de Gestão dos Riscos de Integridade é realizado considerando as seguintes fases:

Identificação dos Riscos

Detecta nos processos da Celesc riscos e fatores de risco relacionados à integridade. Esses riscos irão compor a Árvore de Riscos de Integridade, que é revisada anualmente.

Análise e Avaliação dos Riscos

Procura compreender o risco e fatores de risco, levando em consideração as incertezas, fontes, consequências, eventos, cenários, controles, impacto e probabilidade relacionadas àquele risco ou fator de risco, todos sob aspectos internos e externos.

Tratamento dos Riscos

Os Riscos de Integridade poderão ser aceitos, mitigados, transferidos ou eliminados, considerando-se o apetite de risco da Celesc. Para os Riscos de Integridade que ultrapassam os limites do apetite de risco, a resposta será a adoção de medidas para mitiga-los, transferi-los ou eliminá-los.

Monitoramento dos Riscos

Os riscos são monitorados de forma contínua e periodicamente revisados.

Reporte dos Riscos

Periodicamente, é realizado reporte referente ao tratamento e monitoramento dos Riscos de Integridade, o qual é encaminhado para o Comitê responsável pelos temas de Compliance, que reporta para o Conselho de Administração, seguindo o rito da Celesc, de forma a fornecer informações para a tomada de decisão.

9. RESPONSABILIDADES

A presente Política traz as responsabilidades do Conselho de Administração, do Comitê de Auditoria Estatutário e Diretoria Executiva no processo de Gestão Estratégica de Riscos e Controles Internos. As responsabilidades dos demais níveis envolvidos no processo estão apresentadas em normas internas especificas da empresa.

9.1 CONSELHO DE ADMINISTRAÇÃO - CA

Órgão colegiado encarregado do processo de decisão, proteção e valorização (ISE) de uma organização em relação ao seu direcionamento estratégico e principal componente do sistema de Governança Corporativa, com as seguintes responsabilidades no processo de Gestão Estratégia de Riscos e Controles Internos:

- Aprovar a Política de Gestão Estratégica de Riscos e Controles Internos da Celesc visando o alinhamento com a estratégia da companhia *(CVM 480);*
- Aprovar a estratégia de longo prazo considerando riscos e oportunidades *(DEC 8945);*
- Implementar e supervisionar os sistemas de gestão de riscos e controles internos estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a empresa *(Lei 13303);*
- Discutir, aprovar, monitorar e revisar o apetite e a tolerância a riscos e avaliar se está de acordo com o desempenho da organização *(ISE/IBGC 2017)*;
- Avaliar periodicamente a exposição da companhia a riscos e a eficácia dos sistemas de gerenciamento de riscos e dos controles internos, assim como a disponibilidade de recursos necessários *(CVM 480);*
- Monitorar de forma contínua os riscos que podem impactar os objetivos da organização *(IBGC 2017)*;

- Assegurar que a administração implemente controles efetivos para mitigar os riscos de perdas das informações ou de acessos não autorizados (segurança da informação) (IBGC 2017);

- Estimular o diálogo sobre riscos entre a gestão e o Conselho de Administração (IBGC 2017);

- Definir seu papel e dos comitês de assessoramento na supervisão dos riscos, inclusive delegar atividades para serem realizadas por comitê de assessoramento (IBGC 2017);

- Busca confirmar, por meio da auditoria interna, que as estruturas e processos de governança foram devidamente criados e estejam operando conforme o planejado (IIA);

- Determina o apetite organizacional a riscos e exerce a supervisão do gerenciamento de riscos, incluindo controle interno (IIA).

9.2 COMITÊ DE AUDITORIA ESTATUTÁRIO - CAE

O Comitê de Auditoria Estatutária - CAE é um órgão estatutário de assessoramento vinculado diretamente ao Conselho de Administração das Centrais Elétricas de Santa Catarina S.A. – Celesc, de caráter permanente, ao qual compete:

- Avaliar e monitorar exposições de risco da companhia definidos pelo CA *(DEC 8945 / IBGC 2017);*

- Relatar ao CA a execução das políticas e cumprimento das normas de Gestão de Riscos *(IBGC 2017);*

- Acompanhar os indicadores-chave de riscos e, se for o caso, relatar alertas ao Conselho de Administração para discussão e avaliação de aderência à cultura de riscos da organização *(IBGC 2017);*

- Supervisionar a qualidade e integridade dos processos relativos ao gerenciamento de riscos e ao sistema de controles internos, em linha com as diretrizes estabelecidas pelo CA *(IBGC 2017).*

9.3 DIRETORIA EXECUTIVA

Compete à Diretoria Executiva:

- Promover e intensificar o diálogo com o Conselho de Administração sobre o uso do gerenciamento de riscos corporativos no processo de refinamento da estratégia, promovendo oportunidade de melhorar seu entendimento sobre como a discussão explícita do risco afeta a estratégia *(COSO)*;

- Cabe ao Presidente a responsabilidade final pelo gerenciamento de riscos corporativos, certificando-se de que todos os componentes de Gestão de Riscos e Controles Internos estejam implementados e efetivos *(COSO/IBGC);*

- Avaliar e submeter à aprovação do Conselho de Administração as propostas de limites de riscos;

- Cumprir os limites de apetite de riscos aprovados pelo Conselho de Administração;

- Orientar a aplicação do gerenciamento de riscos perante os gerentes dos departamentos, responsáveis pelo gerenciamento dos riscos, assegurando que essa aplicação é consistente com o apetite e a tolerância ao risco da companhia *(COSO)*;

- Identificar, avaliar, controlar, mitigar e monitorar os riscos aos quais a empresa encontra-se exposta;

- Reportar os riscos identificados ao Comitê de Auditoria Estatutário e ao Conselho de Administração;

- Disseminar a cultura de Gestão de Riscos e Controles Internos;

- Prover os recursos necessários para assegurar a efetividade do Gerenciamento de Riscos Corporativos de Reporte Financeiro e de Integridade *(IBGC 2017);*

- Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos, incluindo controle interno (IIA).

9.4 DEMAIS ENVOLVIDOS

Além das reponsabilidades previstas nos itens 9.1, 9.2 e 9.3 desta Política, devem ser consideradas ainda as responsabilidades sobre Gestão de Riscos e Controles Internos mencionadas nas seguintes normativas internas da Celesc:

- Instrução Normativa I-100.0011 – Processo de Controles Internos para Gestão dos Riscos de Reporte Financeiro

- Instrução Normativa I-100.0012 – Processo de Gestão de Riscos Corporativos

- Instrução Normativa I-100.0020 – Processo de Gestão de Riscos de Integridade

10. DISPOSIÇÕES FINAIS

Os conceitos, princípios e metodologias aplicados a esta Política baseiam-se em normas que norteiam as melhores práticas de mercado e na legislação vigente.

Esta Política deve ser considerada em conjunto com outras normas, padrões e procedimentos aplicáveis às subsidiárias integrais da Celesc S.A., sendo desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes aqui estabelecidas.

Deverão ser submetidas à apreciação do Comitê de Auditoria Estatutário, à Diretoria Executiva e ao Conselho de Administração as exceções, violações e casos omissos a esta Política.

Esta Política foi aprovada pelo Conselho de Administração, conforme registro na Ata da Reunião de 15.10.2020 e possui validade indeterminada.

Dúvidas a respeito da Política de Gestão Estratégica de Riscos e Controles Internos poderão ser esclarecidas pelo Departamento de Gestão de Riscos e Controle Interno – DPGR e/ou pelo Departamento de Compliance – DPCP.

11. REFERÊNCIAS

Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes

COSO ERM – Enterprise Risk Management Framework – *Integrating with Strategy and Performance*

Norma ABNT ISO GUIA 73:2009 – Gestão de Riscos: Vocabulário

Índice de Sustentabilidade Empresarial (ISE) – Bovespa

Gerenciamento de Riscos Corporativos (2017) – IBGC

Código das Melhores Práticas de Gestão Corporativa (2015) – 5º Ed – IBGC

Lei 13.303/16 – Lei das Estatais

Lei 12.846/13 – Lei Anticorrupção

Decreto 8.420/15 – Regulamenta a Lei Anticorrupção

Lei 6.404/76 – Leis das S.A.

RN787/17 – Regulamenta a avaliação da qualidade dos sistemas de governança corporativa a ser aplicada às distribuidoras de energia elétrica – ANEEL

Decreto 1.484/18 – Fixa as diretrizes para a promoção das adaptações necessárias à adequação das empresas públicas e sociedades de economia mista e suas subsidiárias do Estado de Santa Catarina

Lei 17.715/19 – Programa de Integridade e Compliance SC

Managing the Business Risk of Fraud – Association of Certified Fraud Examiners

Guia Prático de Gestão de Riscos para a Integridade – Ministério da Transparência e Controladoria-Geral da União – Outubro de 2018

12. APROVAÇÃO E REVISÕES

Aprovação da primeira edição da Política de Gestão Estratégica de Riscos e Controles Internos da Celesc S.A. em Ata do Conselho de Administração de 18.04.2013.

Primeira Revisão em 15.10.2020.