

1. OBJETIVO E ESCOPO

Esta Orientação visa estabelecer as políticas corporativas, práticas e outros aspectos da Gestão de Riscos na CEITEC S.A., elaborada pela Diretoria de Governança, Risco e Conformidade, tem o objetivo de aperfeiçoar a gestão por parte dos setores responsáveis.

2. RESPONSABILIDADES

Este documento deverá ser mantido e atualizado pela Diretoria de Governança, Risco e Conformidade da CEITEC. Nos processos em que há outras áreas envolvidas, a parte do processo em questão será de responsabilidade dessas áreas.

3. DESCRIÇÃO DO PROCESSO

3.1. Definições

Riscos e Oportunidades: efeitos da incerteza nos objetivos; são fatores, eventos ou condições incertas que, caso concretizadas, podem afetar negativamente (riscos) ou positivamente (oportunidades) algum dos objetivos ou atividades da empresa, de uma área da empresa, de projetos ou ainda de produtos ou serviços, em aspectos como prazo, custo, qualidade, escopo, conformidade e imagem, dentre outros.

Gestão de Riscos: disciplina de gestão que trata da incerteza; é uma maneira organizada de identificar, mensurar e priorizar riscos e oportunidades, bem como desenvolver e implementar estratégias, considerando os níveis desejados pela organização, para aumentar a probabilidade e o impacto dos eventos positivos, e diminuir a probabilidade e o impacto dos eventos adversos.

Apetite para Risco: quantidade, nível ou grau de oportunidade que a organização está preparada para buscar ou de risco que é tolerável, justificável ou julgado aceitável pela organização, no geral, ou em cada contexto considerado.

Gestor de Riscos: Gestor ou outro Colaborador designado pela Diretoria Executiva ou pela Diretoria de Governança, Risco e Conformidade como mantenedor do catálogo corporativo de riscos, responsável pelas ações de educação e capacitação e por garantir que ocorram os processos de identificação, priorização, documentação, tratamento, medição e avaliação dos riscos e oportunidades.

Proprietário do Risco ou Oportunidade: Gestor, Equipe ou Colaborador responsável por gerenciar um item de risco ou de oportunidade, monitorando-o, definir a estratégia de resposta, verificar se a estratégia de resposta está sendo aplicada e está sendo eficaz, e preencher todos os sistemas de informação e relatórios de controles de riscos e oportunidades que lhe forem atribuídos.

Para definições adicionais consulte a Orientação 3.110.002, Vocabulário Controlado de Gestão.

3.2. Gestão corporativa de riscos

- 3.2.1. A atividade econômica da CEITEC é complexa, envolve diversos atores e um alto grau de inovação de produtos, processos e de modelos de negócio, bem como diferentes tipos de relacionamentos com fornecedores, clientes, parceiros de negócio e com a sociedade em geral.

- 3.2.2. A atuação neste cenário traz, naturalmente, muitas incertezas e exige maior convívio e exposição a riscos e busca de oportunidades.
- 3.2.3. Todavia, estes riscos e oportunidades precisam ser mapeados e gerenciados para que se mantenham dentro de um patamar aceitável de acordo com o contexto considerado:
 - 3.2.3.1. Aceitável pelos Colaboradores, que representam o capital humano e intelectual da empresa;
 - 3.2.3.2. Aceitável pelos Gestores de todos os níveis da empresa, que assumem a responsabilidade de conduzir as atividades meio e fim da empresa e têm a necessidade de lidar com a incerteza, devendo levar avaliações dos riscos envolvidos em consideração na tomada de decisões;
 - 3.2.3.3. Aceitável pela alta administração da empresa, representada pela Diretoria Executiva e pelo Conselho de Administração, e que deve garantir a continuidade e prosperidade dos negócios; e
 - 3.2.3.4. Aceitável pelos Investidores, representados pela União, que esperam que a empresa cumpra sua missão empresarial estabelecida em seu Estatuto Social e na Lei 11.759 de 31/07/2008.
- 3.2.4. A Gestão de Riscos busca reconhecer os riscos e capturar as oportunidades, diminuir a probabilidade ou o impacto de eventos adversos à empresa ou às suas áreas e atividades, e aumentar a probabilidade ou impacto de oportunidades para ampliar a geração de valor para a empresa.
 - 3.2.4.1. A Gestão de Riscos é desafiadora, pois alguns riscos não podem ser evitados, algumas oportunidades não podem ser exploradas, e os recursos disponíveis para a Gestão de Riscos são finitos e limitados.
 - 3.2.4.2. Através da priorização dos riscos e oportunidades, pela análise de probabilidade e impacto, pode-se racionalizar o uso dos recursos disponíveis.
- 3.2.5. A CEITEC acredita e está comprometida com a Gestão Corporativa de Riscos porque ela gera valor para a empresa e traz vantagens como:
 - 3.2.5.1. Abre canais oficiais de comunicação que permitem que todos atuem proativamente antevendo e alertando sobre ameaças e oportunidades;
 - 3.2.5.2. Evita a paralisia diante de qualquer risco, pois permite a ação consciente visando a definição de estratégias de mitigação de impacto que fomentam e potencializam decisões adequadas;
 - 3.2.5.3. Contribui para a Gestão de Continuidade de Negócios através do controle e medidas de prevenção de danos;
 - 3.2.5.4. Contribui para a Governança Corporativa aderente aos padrões de conformidade (*compliance*) gerando padrões de operação, controladoria e desempenho;
 - 3.2.5.5. Fortalece a reputação da empresa;
 - 3.2.5.6. Favorece a satisfação do Cliente;
 - 3.2.5.7. Desenvolve a prontidão para mudança;
 - 3.2.5.8. Reduz o esforço dos Gestores no planejamento de ações e controle de eventos não planejados;

- 3.2.5.9. Traz maior eficiência no uso de recursos da empresa já que reconhece e evidencia quais riscos e oportunidades já estão sendo tratados e dispensa a duplicidade de esforços no escopo de outras áreas, atividades e projetos da empresa;
- 3.2.5.10. Evita competição entre áreas pelos recursos disponíveis uma vez que riscos e oportunidades são propagados, consolidados e priorizados no âmbito corporativo e as decisões são tomadas dentro de uma visão estratégica.
- 3.2.6. A Gestão Corporativa de Riscos (ERM, do inglês *enterprise risk management*) na CEITEC deverá se integrar aos processos operacionais, táticos e estratégicos e também às práticas de gestão e à cultura organizacional da empresa, sendo estruturada em vários níveis que permeiam toda a organização:
 - 3.2.6.1. Em seu nível mais fundamental encontramos os catálogos de riscos e oportunidades, planos de ação, atividades e projetos de cada colaborador específico.
 - 3.2.6.2. No nível das equipes responsáveis por um determinado conjunto de tarefas encontramos os catálogos de riscos e oportunidades, planos de ação, atividades e projetos atribuídos a toda equipe de forma compartilhada;
 - 3.2.6.3. Em seu nível gerencial encontramos os catálogos de riscos e oportunidades, planos de ação, atividades e projetos atribuídos a cada nível gerencial específico;
 - 3.2.6.4. Em seu nível mais alto uma visão estratégica e abrangente é oferecida à alta administração da empresa, que tem como foco a governança e continuidade do negócio.
- 3.2.7. Todos os níveis do gerenciamento de riscos são baseados em análise qualitativa e quantitativa e numa nomenclatura comum que tem como objetivo promover maior uniformidade de classificação e interpretação facilitando a agregação de dados.
- 3.2.8. Esta estruturação permite que:
 - 3.2.8.1. Atividades onde se observa inerentemente maior vulnerabilidade ou potencial impacto dos riscos possam ser acompanhadas com maior rigor e desenvolvam maior maturidade no gerenciamento de riscos.
 - 3.2.8.2. Ao longo do tempo, práticas de maior efetividade aplicadas nestas atividades sejam incorporadas à cultura organizacional e propagadas para as demais atividades de empresa.
- 3.2.9. Este processo é estimulado através de quatro elementos principais:
 - 3.2.9.1. Análise qualitativa e quantitativa e nomenclatura comum de classificação de riscos e oportunidades;
 - 3.2.9.2. Responsabilização (*accountability*), por meio da designação de um ou mais Proprietário(s) responsável(eis) pelo monitoramento do item de risco ou oportunidade identificado e pela definição e implementação dos planos de ação de resposta ao risco ou oportunidade;
 - 3.2.9.3. Monitoramento periódico mandatório pelos Gestores de Riscos em seus diferentes níveis; os Gestores de Riscos são também responsável pela promoção da Cultura da Gestão Corporativa de Riscos de forma continuada e sustentada;
 - 3.2.9.4. Avaliação periódica mandatória do sistema de Gestão Corporativa de Riscos pela área de Qualidade da empresa, Auditoria Interna e Diretoria Executiva.

3.3. Admissibilidade de métodos alternativos ou complementares de gerenciamento de riscos

- 3.3.1. É facultado às diversas áreas, atividades ou projetos da empresa, desde que devidamente justificado e previamente aprovado pela Diretoria de Governança, Risco e Conformidade:
 - 3.3.1.1. Adotarem metodologias próprias de análise qualitativas e quantitativa de riscos e oportunidades, julgadas mais adequadas ao seu contexto de aplicação e de acordo com viabilidade técnica, ferramental e capacitação da equipe;
 - 3.3.1.2. Adotarem outros critérios ou outra nomenclatura de classificação de riscos e oportunidades, conforme seja mais adequado à natureza da atividade realizada.
- 3.3.2. Ao adotar qualquer método de análise, critério ou nomenclatura diferentes do padrão corporativo, torna-se mandatário que os resultados desta análise venham sempre reinterpretados ou convertidos pela própria área, atividade ou projeto para a nomenclatura comum corporativa de classificação da análise qualitativa para fins de compartilhamento através dos meios de registro e comunicação previstos no processo de Gestão Corporativa de Riscos.

3.4. Plano de Gestão Corporativa de Riscos

- 3.4.1. Os Gestores de Riscos designados pela Diretoria Executiva ou pela Diretoria de Governança, Risco e Conformidade são responsáveis por emitir e manter o Plano de Gestão Corporativa de Riscos.
- 3.4.2. O Plano de Gestão Corporativa de Riscos terá vigência até sua revogação por meio da aprovação pela Diretoria Executiva de um novo plano que o substitua, ou atualize.
- 3.4.3. O Plano de Gestão Corporativa de Riscos será submetido para análise e aprovação da Diretoria Executiva, e entrará em vigor a partir da data de sua aprovação e disponibilização na intranet da empresa.
- 3.4.4. Ressalvada orientação em contrário da Diretoria Executiva, o Plano de Gestão Corporativa de Riscos será publicado no Portal Corporativo após a aprovação, para conhecimento de todos os Gestores, demais Colaboradores e outras Partes Interessadas, com publicação divulgada através do Comunicado Interno conforme Procedimento Operacional 3.120.001.
- 3.4.5. O Plano de Gestão Corporativa de Riscos deverá apresentar os seguintes aspectos:
 - 3.4.5.1. Ferramentas e metodologias que serão adotadas na Gestão de Riscos no período de vigência do plano;
 - 3.4.5.2. Parâmetros monitorados, indicadores, benefícios, orçamento, metas, apetite para risco, critérios, condições, limites e alçadas relevantes para a Gestão de Riscos que estarão em efeito ao longo do período;
 - 3.4.5.3. Detalhamento das ações de capacitação a serem realizadas, incluindo calendário e matriz de responsabilidades;
 - 3.4.5.4. Calendário de atividades de gerenciamento de riscos;
 - 3.4.5.5. Detalhamento do calendário de auditorias e matriz de responsabilidades.

3.5. Acompanhamento

- 3.5.1. Serão emitidos relatórios corporativos consolidados de acompanhamento de riscos agregando as informações fornecidas pelas diferentes fontes de informação dos diversos níveis de gestão da empresa (como definido na Seção 3.2.6) e apurando as informações relevantes no escopo do nível mais alto de visão estratégica (como definido na Seção 3.2.6.4).
 - 3.5.1.1. O relatório de acompanhamento será distribuído para os membros da Diretoria Executiva, do Conselho de Administração, do Conselho Fiscal e do Comitê de Auditoria.
 - 3.5.1.2. Para atender seus objetivos de informação desse público alvo, o nível de detalhes do relatório de acompanhamento deve ser ajustado para garantir uma comunicação eficaz, no sentido de que as informações são fornecidas no formato correto, no tempo adequado e com o impacto necessário, e eficiente, no sentido de fornecer somente as informações que são necessárias e mais relevantes.
 - 3.5.1.3. A emissão do relatório de acompanhamento é de responsabilidade dos Gestores de Riscos designados pela Diretoria Executiva ou pela Diretoria de Governança, Risco e Conformidade.
 - 3.5.1.4. Serão emitidos pelo menos um relatório completo por ano e relatórios resumidos trimestrais.
 - 3.5.1.5. Esses relatórios serão emitidos em datas que serão definidas no calendário de atividades que é parte do Plano de Gestão Corporativa de Riscos conforme Seção 3.4 deste documento.
 - 3.5.1.6. Os Gestores de Riscos poderão emitir relatórios de acompanhamento ou outras comunicações a qualquer tempo que julgarem necessário, desde que previamente aprovados em termos de seu conteúdo e destinatários, pela Diretoria de Governança, Risco e Conformidade, ou que se enquadrem nos casos que essa Diretoria já tenha definido como de comunicação urgente, de modo a atender os princípios de oportunidade e proatividade da Gestão de Riscos.

3.6. Capacitação e educação

- 3.6.1. Todos os membros da Diretoria Executiva têm a obrigação de conhecer os dois documentos que definem o processo de Gestão Corporativa de Riscos na CEITEC, que são esta Orientação 1.110.002, Política de Gestão de Riscos, e o Procedimento Operacional 3.110.005, Gestão Corporativa de Riscos.
 - 3.6.1.1. A capacitação do Diretor de Governança, Risco e Conformidade e dos demais diretores da Diretoria Executiva poderá ser realizado por meio de diferentes iniciativas, conforme a conveniência de cada caso, incluindo autoinstrução, grupo de estudo ou ensino mútuo, estudo dirigido individual ou em grupo com o apoio de instrutor, ou ainda aulas expositivas com apoio de instrutor organizadas em turmas.
 - 3.6.1.2. Considera-se qualificado como instrutor de treinamento qualquer pessoa previamente capacitada neste mesmo conteúdo.
 - 3.6.1.3. Os autores e aprovadores dos documentos serão considerados implicitamente capacitados, dispensando o treinamento.
- 3.6.2. A identificação da necessidade de treinamento dos Gestores e demais Colaboradores, o registro de treinamento e o mapeamento de competências deverão ser conduzidos conforme o Procedimento

Operacional 3.210.023 Levantamento de Necessidades de Treinamento e o Procedimento Operacional 3.310.002, Elaboração de Documentos do Sistema de Gestão da Qualidade.

- 3.6.3. Com o objetivo de promover a sedimentação da gestão de riscos na cultura organizacional, ações adicionais de divulgação, treinamento, educação e conscientização dos Gestores e demais Colaboradores em relação à Gestão Corporativa de Riscos devem ser implementadas periodicamente.
- 3.6.3.1. Estas ações serão coordenadas pelo Gestores de Riscos designados pela Diretoria Executiva ou pela Diretoria de Governança, Risco e Conformidade e poderão ser concretizadas através de palestras, workshops com estudos de casos, autoinstrução ou outras ações de desenvolvimento de capacitação definidas pelo Gestor de Riscos designado.
 - 3.6.3.2. Estas ações serão avaliadas através de questionário de autoavaliação, com foco na aprendizagem e impacto na organização, e avaliação de reação, com foco na satisfação dos participantes, e seus registros serão mantidos para fins de auditoria.
 - 3.6.3.3. Os Gestores de Riscos designados serão responsáveis pela consolidação e análise estatística dos questionários e emissão de um relatório de avaliação das ações de capacitação e educação que será encaminhado para a Diretoria de Governança, Risco e Conformidade.
 - 3.6.3.4. O relatório de avaliação das ações de capacitação e educação será emitido e divulgado anualmente em data definida no calendário de atividades que é parte do Plano de Gestão Corporativa de Riscos conforme Seção 3.4 deste documento.

3.7. Auditoria e conformidade

- 3.7.1. Auditorias de conformidade dos processos de Gestão Corporativa de Riscos serão executadas pela área da Qualidade, conforme Procedimento Operacional 2.300.005, Auditoria Interna da Qualidade.
- 3.7.1.1. Será executada pelo menos uma auditoria por ano, abrangendo pelo menos esta Orientação 1.110.002, Política de Gestão de Riscos, e o Procedimento Operacional 3.110.005, Gestão Corporativa de Riscos.
 - 3.7.1.2. A auditoria anual será realizada em data acordada com a área da Qualidade e o detalhamento e calendário das atividades de auditoria de conformidade dos processos constarão no Plano de Gestão Corporativa de Riscos conforme Seção 3.4 deste documento.
- 3.7.2. A análise crítica dos relatórios de auditoria de conformidade dos processos, dos relatórios de avaliação anual das ações educacionais e dos relatórios corporativos consolidados de acompanhamento será realizada pela área de Auditoria Interna da CEITEC, que emitirá parecer considerando a conformidade dos processos (conforme Seção 3.7.1), efetividade das ações educacionais (conforme Seção 3.6.3.2) e a eficácia e eficiência da comunicação (conforme Seção 3.5.1.2).
- 3.7.2.1. A análise crítica dos relatórios será realizada em data acordada com a área de Auditoria Interna que constará no calendário de atividades que é parte do Plano de Gestão Corporativa de Riscos conforme Seção 3.4 deste documento.

3.8. Visão e compromissos de melhoria

3.8.1. A CEITEC estabelece como compromissos futuros e ações de melhoria na Gestão Corporativa de Riscos:

- 3.8.1.1. Contar com profissionais qualificados designados como Gestores de Riscos com capacitação para a Gestão de Riscos Corporativos em conformidade com o padrão ABNT NBR ISO 31000;
- 3.8.1.2. Aperfeiçoar e adequar o seu sistema de Gestão Corporativa de Riscos, onde pertinente, ao padrão ABNT NBR ISO 31000 de Gestão de Riscos e aos Princípios de Governança Corporativa da Organização para a Cooperação e Desenvolvimento Econômico (OCDE/OECD);
- 3.8.1.3. Integrar a Gestão Corporativa de Riscos como fonte de informação para as práticas corporativas de Gestão de Continuidade de Negócios conforme padrão ABNT NBR ISO 22301;
- 3.8.1.4. Capacitação dos Gestores para atuar proativamente antevendo e alertando sobre ameaças e oportunidades e para lidar com incerteza, imprevisibilidade, mudança e instabilidade, integrando os riscos e oportunidades no processo decisório, de modo a viabilizar, fomentar e potencializar a inovação necessária para o crescimento futuro da empresa.

3.8.2. Estes compromissos e ações deverão se concretizar até dezembro de 2020.

3.9. Aprovação, vigência e atualização

Esta revisão da Política de Gestão de Riscos foi aprovada pelo Conselho de Administração em 29 de agosto de 2018. Nova revisão ocorrerá anualmente, conforme deliberação do Conselho de Administração de 19 de agosto de 2016.

4. PADRÕES/FORMULÁRIOS ASSOCIADOS

- Não aplicável.

5. CONTROLE DE REGISTROS

- Não aplicável.

6. DOCUMENTOS ASSOCIADOS

- OR 3.110.002 Vocabulário Controlado de Gestão;
- PO 3.110.005 Gestão Corporativa de Riscos.