POLÍTICA DE GESTÃO DE RISCOS

2024

SUMÁRIO

1. INTRODUÇÃO

A presente **Política de Gestão de Riscos (PGR)** está alinhada com a Política Estadual de Gestão de Riscos do Poder Executivo do Estado do Ceará e estabelece diretrizes, princípios, responsabilidades e orientações relativos ao gerenciamento de riscos para a Empresa de Tecnologia da Informação do Ceará – Etice.

2. OBJETIVO

O objetivo desta política é dar suporte à governança corporativa e aprimorar o controle interno, visando prevenir ou minimizar os riscos que podem impactar no alcance de seus resultados e no cumprimento da sua missão, protegendo e promovendo os interesses da organização e de suas partes interessadas.

3. ABRANGÊNCIA

Esta política deverá ser aplicada por todos os administradores, empregados e colaboradores da empresa, incluindo ocupantes de cargo em comissão, servidores públicos em disposição funcional ou cedidos, bem como empregados terceirizados, prestadores de serviços e estagiários.

4. INSTRUMENTOS LEGAIS E NORMATIVOS

Lei Federal nº 13.303/2016 – DISPOSIÇÕES APLICÁVEIS ÀS EMPRESAS PÚBLICAS E ÀS SOCIEDADES DE ECONOMIA MISTA (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm);

Decreto Estadual nº 33.805/2020 – POLÍTICA DE GESTÃO DE RISCOS DO PODER EXECUTIVO DO CEARÁ (cge.ce.gov.br/wp-content/uploads/sites/20/2020/11/Decreto-33805-2020-Politica-de-Gestao-de-Riscos-do20201110p01.pdf);

Portaria nº 05/2021 da CGE – METODOLOGIA DE GERENCIAMENTO DE RISCOS DO PODER EXECUTIVO DO CEARÁ (do20210209p01 - PORTARIA Nº05/2021. (cge.ce.gov.br));

Norma ABNT ISO 31.000/2009 – GESTÃO DE RISCOS (http://www.abnt.org.br/imprensa/releases/5828-abnt-publica-a-versao-abnt-nbr-iso-31000-gestao-de-riscos);

Lei Estadual nº 16.717/2018 – PROGRAMA DE INTEGRIDADE DO PODER EXECUTIVO DO CEARÁ LEI N.º 16.717, DE 21.12.18 (D.O. 26.12.18) (al.ce.gov.br);

Decreto Estadual nº 32.243 de 31 de maio de 2017 – APLICAÇÃO, NO ÂMBITO ESTADUAL, DA LEI FEDERAL Nº13.303, DE 30 DE JUNHO DE 2016, PARA AS EMPRESAS PÚBLICAS E SOCIEDADES DE ECONOMIA MISTA DO ESTADO DO CEARÁ DE MAIOR RECEITA OPERACIONAL Decreto-Estadual-32.243-de-31-de-maio-de-2017.pdf (cge.ce.gov.br);

Decreto Estadual nº 32.792/2018 – DISTRIBUIÇÃO E DENOMINAÇÃO DOS CARGOS DE PROVIMENTO EM COMISSÃO DA EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ – ETICE Novo-Estatuto-da-Etice.pdf;

5. DEFINIÇÕES

Os seguintes termos e definições relacionados à Gestão de Riscos têm como base o Art. 3º do Decreto nº 33.805 de 09/11/2020 DOE 10/11/2020 (institui a Política de Gestão de Riscos do Poder Executivo do Estado do Ceará), bem como a Norma ABNT NBR – ISO 31000:2009, e visam assegurar uma compreensão comum para todos:

Análise: aplicada ao processo de gerenciamento de riscos, aos eventos de riscos ou às medidas de tratamento/controle: atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir objetivos estabelecidos.

Análise de Riscos: a análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.

Avaliação de Riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

Consequências: resultados de um evento que podem afetar positiva ou negativamente os objetivos da organização. As consequências podem ser expressas qualitativa ou quantitativamente e consequências iniciais podem inclusive desencadear reações em cadeia (efeito dominó).

Contexto: pode ser **Externo:** pode incluir o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, regional ou local, bem como os fatores-chaves e as tendências que tenham impacto sobre os objetivos da organização, as relações com partes interessadas externas e suas percepções e valores: ambiente externo no qual a organização busca atingir seus objetivos. ou pode der **Interno:** pode incluir governança, estrutura organizacional, funções e responsabilidades; políticas, objetivos e estratégias implementadas para atingi-los; capacidades compreendidas em termos de recursos e conhecimentos (por exemplo: capital, tempo, pessoas, processos, sistemas e tecnologias); sistemas de informação, fluxos de informação e processos de tomada de decisão (formais/informais); relações com partes interessadas internas, suas percepções e valores; cultura da organização; normas, diretrizes e modelos adotados pela organização; forma e extensão das relações contratuais (ambiente interno e externo) no qual a organização busca atingir seus objetivos.

Controle Interno: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, processos e trâmites de documentos e informações operacionalizados de forma integrada, destinados a identificar, enfrentar e mitigar os riscos, a fim de fornecer transparência e segurança razoáveis para que os objetivos organizacionais da empresa sejam alcançados.

Estrutura: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua do gerenciamento de riscos de toda a organização.

Evento de Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização.

Gerenciamento de Riscos: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos, processos de trabalho e projetos da organização.

Gestão de Riscos: conjunto de ações coordenadas e direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento dos riscos institucionais mais críticos, objetivando apoiar a melhoria contínua de processos estratégicos da

organização, visando alcançar seus objetivos estratégicos, com maior eficácia na alocação e utilização dos recursos disponíveis.

Governança: o conjunto de mecanismos de liderança, estratégia e controle postos em prática para informar, dirigir, administrar, avaliar e monitorar as atividades organizacionais, com o intuito de alcançar seus objetivos e garantir uma conduta transparente, ética e responsável.

Identificação de Riscos: processo de busca, catalogação e descrição dos riscos (fontes de riscos, eventos, causas e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas/especialistas e as necessidades das partes interessadas).

Impacto: efeito resultante da ocorrência do evento de risco.

Monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. O monitoramento pode ser aplicado à estrutura da Gestão de Riscos, ao processo de Gerenciamento de Riscos, ao risco propriamente dito, e aos controles.

Nível de Riscos: grau de criticidade dos riscos, assim compreendida a intensidade do impacto de um risco nos objetivos, processos de trabalho e organização, a partir de uma matriz de referência pré-definida.

Objetivo Estratégico: situação que se deseja alcançar de forma a evidenciar um êxito considerável no cumprimento da missão e no atingimento da visão de futuro na organização.

Partes Interessadas: pessoas ou organizações que podem afetar, ser afetadas, ou se perceber afetadas por uma decisão ou atividade de determinada organização.

Política de Gestão de Riscos (PGR): declaração das intenções e diretrizes gerais referentes ao gerenciamento dos riscos considerados mais críticos para os processos críticos da organização/instituição/empresa.

Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido.

Processo de Gerenciamento de Riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

Apetite/Tolerância aos Riscos: níveis de exposição aos riscos que a organização está disposta a assumir, a fim de alcançar seus objetivos.

Tratamento/Controle dos Riscos: abordagem da organização para avaliar e eventualmente mitigar, compartilhar, evitar ou aceitar os riscos.

Plano de Contingência: desenvolvido com o intuito de desenvolver, avaliar, uniformizar, organizar, orientar as ações necessárias para as respostas de controle e combate às ocorrências anormais e adversas.

Probabilidade: chance de um evento de risco ocorrer.

6. PRINCÍPIOS DE GESTÃO DE RISCOS

Os princípios da Política de Gestão de Riscos da Etice que orientam a abordagem eficaz e sustentável para a Gestão de Riscos, fortalecendo sua resiliência e capacidade de enfrentar desafios futuros são os seguintes:

Comprometimento da Alta Administração: Os administradores da Etice devem demonstrar um compromisso claro e contínuo com a Gestão de Riscos, integrando-a nas práticas cotidianas e nas decisões estratégicas.

Abordagem Integrada: A Gestão de Riscos deve ser integrada aos processos de tomada de decisão e à estrutura organizacional, sendo considerada uma parte natural e essencial das atividades diárias.

Identificação Proativa de Riscos: A Etice deve ter sistemas e processos para identificar proativamente os riscos potenciais que possam afetar seus objetivos estratégicos, operacionais e financeiros.

Avaliação Abrangente: Os riscos devem ser avaliados em termos de sua probabilidade de ocorrência e impacto potencial. A avaliação deve levar em conta tanto os riscos individuais quanto os inter-relacionamentos entre eles.

Comunicação Eficaz: Devem existir canais claros e eficazes de comunicação de informações sobre riscos em toda a organização, garantindo que todas as partes interessadas estejam cientes dos riscos relevantes.

Definição de Responsabilidades: As responsabilidades para a Gestão de Riscos devem ser claramente definidas, assegurando que as pessoas certas estejam envolvidas na identificação, avaliação e mitigação dos riscos.

Adoção de Abordagens de Mitigação: Devem ser implementadas estratégias eficazes para diminuir as causas ou as consequências dos riscos conforme apropriado. Isso pode incluir o desenvolvimento de planos de contingência.

Monitoramento Contínuo: A Etice deve monitorar continuamente o ambiente de riscos para identificar mudanças nas condições que possam impactar os riscos identificados, garantindo que as estratégias de mitigação permaneçam eficazes.

Aprendizado Contínuo: A Etice deve aprender com experiências passadas, avaliações de riscos anteriores e eventos inesperados, ajustando sua abordagem de Gestão de Riscos conforme necessário.

Melhoria Contínua: A Política de Gestão de Riscos deve ser revisada periodicamente para garantir sua relevância contínua e ser ajustada à medida que a Etice evolui, garantindo uma abordagem de melhoria contínua.

7. DIRETRIZES

A Etice para a implementação desta política, se norteará pelas seguintes diretrizes:

a) Garantir que a Gestão de Riscos se torne parte importante da cultura da empresa, proporcionando uma atuação proativa de forma a mitigar, compartilhar, evitar e aceitar os riscos para que incertezas não venham a impactar negativamente a execução dos seus objetivos estratégicos.

b) Assegurar os recursos necessários para a implementação de uma metodologia de gerenciamento de riscos, elaborada em conformidade com as melhores práticas internacionais (COSO II ERM, ABNT NBR ISO 31000), adaptada às necessidades e condições da Etice, com destaque para as seguintes ações:

• Trabalhar de forma a antecipar ações que minimizem os efeitos de possíveis eventos que possam afetar o atingimento dos objetivos nos diversos níveis da organização.

• Utilizar a Gestão de Riscos como parte integrante de um processo contínuo de melhoria da Governança Organizacional, garantindo razoável segurança para a realização das atividades rotineiras.

• Realizar o tratamento adequado dos riscos, agregando valor à empresa e propiciando a redução dos impactos negativos decorrentes de possível materialização desses eventos, auxiliando na melhoria do processo de tomadas de decisão.

• Capacitar os funcionários, por meio de treinamentos específicos que abordem, de forma clara e objetiva, as responsabilidades, os principais instrumentos e ferramentas de Gestão de Riscos adotados pela empresa, buscando aprimorar e unificar a linguagem e o conhecimento em toda a Etice.

8. ESTRUTURA DE GESTÃO DE RISCOS

A estrutura de Gestão de Riscos deve propiciar um amplo engajamento de todos os níveis de atuação da empresa na implementação da Gestão de Riscos, dentre eles, Presidente, Diretores, Gerentes, responsáveis pelos processos nas diversas unidades organizacionais, para o cumprimento dos objetivos estratégicos, dos processos e ações primordiais, a fim de assegurar maior eficiência na performance geral da empresa.

A Etice deverá implementar e melhorar continuamente sua estrutura interna, visando integrar suas principais atividades, de forma a favorecer a eficácia do gerenciamento de riscos estratégicos e assegurar que aqueles mais críticos sejam adequadamente registrados, classificados e devidamente priorizados para tratamento, a fim de nortearem as tomadas de decisões da alta gestão, em todos os níveis aplicáveis, nas respectivas áreas de atuação, ou sejam, área estratégica, tática e operacional.

9. RESPONSABILIDADES

O gerenciamento de riscos contemplará as seguintes áreas de atuação:
I – estratégica;
II – tática; e
II – operacional.

A **Área de atuação Estratégica,** comitê executivo da Etice ou outra instância de decisão colegiada, definirá as estratégias de implementação do gerenciamento de riscos, considerando os contextos externo e interno da empresa, a fim de:

a) avaliar a eficácia dos controles internos já existentes, em relação aos objetivos estratégicos da empresa, para os processos organizacionais selecionados;

b) analisar e validar a efetividade das medidas de tratamento/controle já existentes, para os processos organizacionais críticos da empresa, a fim de melhorar desempenho de sua Gestão de Riscos e fortalecer a aderência das áreas de atuação da empresa à conformidade normativa estabelecida;

c) aprovar/revisar a seleção dos processos críticos por parte dos gestores das respectivas áreas de atuação, bem como: os níveis de tolerância/apetite aos riscos elencados para estes processos, os indicadores de desempenho relacionados aos riscos priorizados e a periodicidade do ciclo de gerenciamento de riscos.

d) avaliar e validar o resultado do processo de gerenciamento de riscos de cada processo organizacional selecionado;

e) aprovar o plano de comunicação e consulta de gerenciamento de riscos;

A **Área de atuação Tática,** área responsável pelo controle interno da Etice**,** terá como principais funções:

a) auxiliar na identificação dos objetivos estratégicos da organização e na compreensão dos contextos externo e interno a serem considerados no gerenciamento de riscos;

b) auxiliar na identificação, análise e avaliação dos riscos a serem classificados e priorizados para os processos organizacionais selecionados como críticos;

c) auxiliar na definição das respostas aos riscos e das medidas de tratamento e controle a serem implementadas nos processos organizacionais (Plano de Tratamento);

d) auxiliar na definição dos indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da Etice;

e) propor o plano de comunicação e consulta de gerenciamento de riscos;

f) propor a atualização das estratégias de gerenciamento de riscos, considerando os contextos externo e interno;

g) propor a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;

h) realizar o monitoramento e a análise crítica dos níveis de riscos e da efetividade das medidas de tratamento e controle implementadas nos processos organizacionais;

i) auxiliar na definição dos níveis de apetite a riscos dos processos organizacionais;

j) auxiliar na identificação dos responsáveis pelo gerenciamento de riscos dos processos organizacionais;

k) avaliar os indicadores de desempenho para a Gestão de Riscos objetivando melhoria contínua;

l) requisitar aos responsáveis as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;

m) acompanhar o desempenho do processo de gerenciamento de riscos e estimular o fortalecimento da aderência dos processos críticos à conformidade normativa;

n) documentar e informar às outras áreas de atuação cada etapa do processo de gerenciamento de riscos.

As **Áreas de atuação Operacional,** responsáveis pelos processos organizacionais e seus colaboradores terão como principais funções:

a) identificar os objetivos da organização e compreender os contextos externo e interno a serem considerados na Gestão de Riscos;

b) identificar, analisar e avaliar os riscos dos processos organizacionais selecionados para a implementação do gerenciamento de riscos;

c) definir os níveis de apetite a risco dos processos organizacionais selecionados;

d) propor as respostas aos riscos e as medidas de tratamento e controle a serem implementadas nos processos organizacionais (Plano de Tratamento);

e) monitorar os níveis de riscos e a efetividade das medidas de tratamento e controle implementadas nos processos organizacionais sob sua responsabilidade;

f) informar à área de atuação tática sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;

g) propor os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da Etice;

h) responder às requisições da área de atuação tática;

i) disponibilizar as informações quanto ao gerenciamento de riscos dos processos sob sua responsabilidade a todos os níveis da organização e demais partes interessadas;

j) realizar outras atividades correlatas ao gerenciamento de riscos para os processos sob sua responsabilidade, se necessário.

10. PROCESSO DE GERENCIAMENTO DE RISCOS

O processo de Gerenciamento de Riscos deve abranger etapas, desde a identificação até o monitoramento contínuo, incluindo métodos de avaliação de riscos, critérios de aceitação e estratégias de resposta.

10.1 IDENTIFICAÇÃO DE RISCOS

Os métodos e ferramentas utilizados para identificar riscos, devem incluir análise dos ambientes interno e externo, avaliação de ameaças e oportunidades, entendimento claro sobre riscos, análise sobre quais deles a Etice estará disposta a tolerar (tolerância/apetite a riscos), a fim de determinar aqueles mais críticos e que precisarão ser mitigados, compartilhados, evitados e aceitos prioritariamente.

10.2 AVALIAÇÃO DE RISCOS

Uma vez identificados os riscos a serem analisados, devem ser utilizados os critérios e métodos definidos para avaliar a probabilidade, o impacto dos riscos, no caso de potenciais eventos positivos (oportunidades) ou eventos negativos (riscos), venham a ocorrer, categorizando-os, conforme sua criticidade, para consecução dos objetivos estratégicos da organização.

É importante destacar que não fará sentido gastar recursos para gerenciar riscos que não possuam tanta relevância para o negócio da empresa e para seus objetivos estratégicos, levando sempre em consideração os impactos e custos dos riscos elencados e priorizados para os processos críticos selecionados, em cada caso analisado e em seu contexto próprio.

10.3. TRATAMENTO DE RISCOS

Esta etapa define as estratégias de resposta aos riscos, incluindo opções de tratamento e controle, prevendo as condições para mitigar, compartilhar, evitar e aceitar os riscos priorizados, segundo cada processo abordado. Assim, cada risco crítico deverá estar relacionado a uma medida de tratamento/controle, correspondente ao nível dos riscos classificados.

10.4. REGISTRO E RELATO DE RISCOS

A Fase de Registro será executada por meio de artefatos padronizados e apropriados para fornecer informações essenciais sobre os riscos elencados e priorizados, facilitando assim as tomadas de decisão posteriores para tratamento e controle dos riscos mais críticos pelos gestores da empresa. Esta fase também é importante para que as decisões relativas à criação, retenção e manuseio de informações documentadas possam levar em consideração o seu uso, a sensibilidade da informação e os contextos interno e externo. Frequentemente, a documentação do processo de gerenciamento de riscos é exigida para demonstrar conformidade com requisitos legais ou para mostrar a devida diligência.

A gestão dos riscos deve estabelecer os mecanismos de comunicação interna e externa incluindo a periodicidade dos relatórios e as partes interessadas envolvidas. Cada etapa do processo de gerenciamento de riscos deve ser documentada e comunicada para posterior tratamento e controle dos riscos priorizados pela área responsável.

10.5. MONITORAMENTO E REVISÃO

A Fase de Monitoramento envolverá a verificação e supervisão contínuas, após a elaboração de matriz de riscos para o processo selecionado, visando identificar eventuais mudanças ou adições futuras no desempenho requerido ou esperado para determinar sua adequação, suficiência e eficácia quanto ao gerenciamento de riscos na empresa.

10.6. TREINAMENTO E CONSCIENTIZAÇÃO

O processo de Gerenciamento de Riscos deve prever iniciativas de treinamento para garantir que os colaboradores da organização compreendam e estejam engajados na execução das atividades do processo.

10.7. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

Esta Política de Gestão de Riscos deve ser revisada e atualizada periodicamente, para assegurar sua eficácia contínua diante das mudanças no ambiente operacional e nos objetivos organizacionais.

11. VIGÊNCIA E APROVAÇÃO

Esta política terá sua vigência iniciada após sua aprovação pelo Conselho de Administração.

12. DISPOSIÇÕES FINAIS

A elaboração desta política constitui um marco importante na trajetória da Etice, sendo mais um passo para sua aderência à Lei nº 13.303 de 30 de junho de 2016 – Lei das Estatais, e às melhores práticas nacionais e internacionais de governança.

Fortaleza, 11 de janeiro de 2024

Luis Eduardo Fontenelle Barros
CONSELHEIRO PRESIDENTE

ASSINADO DIGITALMENTE
JOSE VALDECI REBOUCAS
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

José Valdeci Rebouças
CONSELHEIRO

José Juarez Diógenes Tavares
CONSELHEIRO

Alfredo José Pessoa de Oliveira
CONSELHEIRO

Documento assinado digitalmente
gov.br
DEBORAH VANESSA RIBEIRO BARBOSA CAMARA
Data: 18/01/2024 14:05:47-0300
Verifique em https://validar.iti.gov.br

Déborah Vanessa Ribeiro Barbosa Câmara
CONSELHEIRA