POLÍTICA DE GESTÃO DE RISCOS

OBJETO

A Política de Gestão de Riscos ("Política") da Companhia de Engenharia de Tráfego ("CET") tem o propósito de estabelecer as regras de estruturas e práticas de gestão de riscos e controle interno, de maneira geral e transparente, consoante normas legais e estatutárias em vigor.

DISPOSIÇÕES APLICÁVEIS

Diretrizes

1. A presente "Política" integra o Programa de Integridade da CET e busca garantir o cumprimento do disposto no artigo 9º, seus incisos e parágrafos, da Lei Federal nº 13.303, de 30 de junho de 2016, estabelecendo o posicionamento da empresa diante de eventuais riscos que possam ameaçar o alcance dos objetivos organizacionais e ou prejudicar a sua imagem e reputação.
2. Consoante a norma ABNT NBR ISO 31000:2009, da Associação Brasileira de Normas Técnicas (ABNT), a política de gestão de riscos caracteriza-se na "declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos", devendo especificar:
   2.1. Objetivos organizacionais em relação à gestão de riscos;
   2.2. Integração da gestão de riscos a processos e políticas organizacionais;
   2.3. Responsabilidade por gerenciar riscos;
   2.4. Diretrizes sobre como identificar, avaliar, tratar e monitorar os riscos;
   2.5. Fluxo de comunicação e consultas, internas e externas, sobre assuntos relacionados a riscos;
   2.6. Diretrizes para a medição do desempenho da gestão de riscos;
   2.7. Análise crítica e aperfeiçoamento da política e das estruturas de gestão de riscos em resposta a um evento ou mudança nas circunstâncias.

Definições e práticas

3. **Conceituação de risco**: evento futuro e incerto que, caso ocorra, pode impactar negativamente o alcance dos objetivos da empresa.
   3.1. O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades.
4. **Origem dos eventos**: determinar a origem dos eventos (externos ou internos) que representam riscos é importante, pois auxilia na definição da abordagem a ser empregada por parte da empresa.
   4.1. *Riscos externos*: são ocorrências associadas ao ambiente macroeconômico (tecnologias emergentes, ações da concorrência), político (mudança no cenário político), social (conflitos sociais), natural (aquecimento global, catástrofes ambientais) ou setorial (atos terroristas, problemas de saúde pública), em que a empresa opera. A empresa, em geral, não consegue intervir diretamente sobre tais eventos e terá, portanto, uma ação predominantemente reativa, devendo estar bem preparada para essa ação.

4.2. *Riscos internos*: são eventos originados na própria estrutura da empresa, pelos seus processos, seu quadro de pessoal ou de seu ambiente de tecnologia. A empresa pode e deve, em geral, interagir diretamente com uma ação pró-ativa.

5. **Natureza dos riscos**: os riscos aos quais a empresa pode estar sujeita classificam-se, de acordo com a sua natureza, em: estratégicos, operacionais, financeiros, regulatórios e cibernéticos.
   5.1. *Riscos estratégicos*: estão associados à tomada de decisão da alta administração e podem gerar prejuízo econômico à empresa.
   5.2. *Riscos operacionais*: estão associados à possibilidade de ocorrência de perdas (de produção, ativos, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e atos terroristas, com impacto negativo na imagem e reputação da empresa.
   5.3. *Riscos financeiros*: estão associados à exposição das operações financeiras da empresa, tais como a administração financeira inadequada, que conduz a endividamento elevado.
   5.4. *Riscos regulatórios*: também conhecidos como riscos de *compliance* (de conformidade), estão associados à falta de habilidade ou disciplina da empresa para cumprir com a legislação e ou regulamentação externa aplicáveis ao seu negócio e às normas e procedimentos internos.
   5.5. *Riscos cibernéticos*: estão associados às falhas, indisponibilidade ou obsolescência de equipamentos e instalações, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da empresa, ao longo da sua cadeia de valor (fornecedores, parceiros, unidades orgânicas e usuários dos serviços prestados).

6. **Objetivos organizacionais em relação à gestão de riscos**: o Conselho de Administração da CET é o responsável por determinar os objetivos estratégicos da empresa e o perfil de risco aceitável pela para alcançar tais objetivos.
   6.1. Os objetivos estratégicos são definidos por meio do Planejamento Estratégico, instrumento de gestão que contempla o conjunto medidas estratégicas (ações, programas ou projetos) e seus respectivos planos de ação, organizados e ordenados sob os pontos de vista físico e econômico-financeiro.
   6.2. O *perfil de risco* significa em quanta exposição ao risco se aceita incorrer, o que envolve tanto o nível de apetite, quanto o de tolerância a riscos.
   6.3. *Apetite ao risco* está associado ao nível de risco que a empresa pode aceitar na busca e realização de sua missão/visão.
   6.4. *Tolerância ao risco* diz respeito ao nível aceitável de variabilidade na realização das metas e objetivos definidos, sendo uma atividade mais associada ao monitoramento.
   6.5. O perfil de risco deverá estar refletido na cultura da empresa, cabendo ao Conselho de Administração outorgar um mandato claro para a Diretoria administrá-lo.
   6.6. Os riscos corporativos identificados devem ser conhecidos por toda a empresa e, portanto, devidamente comunicados pela Diretoria.

7. **Integração da gestão de riscos a processos e políticas organizacionais**: todas as atividades da empresa serão realizadas de acordo com as exigências legais, os

normativos internos e as boas práticas governamentais e de mercado, mediante o comprometimento com os altos padrões de integridade e valores éticos determinados no Código de Conduta e Integridade.

8. **Responsabilidade por gerenciar riscos**: compete à Diretoria identificar, preventivamente, por meio de sistema de informações adequado, e listar os principais riscos aos quais a empresa está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização.
   8.1. O entendimento e alinhamento dos conceitos relacionados a riscos, bem como a formação de um linguajar comum constituem a gênese da cultura de gerenciamento de riscos, devendo-se implantar o que melhor se aplica à realidade empresa, no contexto em que se encontra e atua.
   8.2. Os riscos corporativos serão, em sua diversidade, controlados e mitigados no âmbito geral, mediante o envolvimento de todos os níveis da empresa, a partir da delegação da responsabilidade pelo seu gerenciamento, de forma clara e formal, à Gerência de Controle Interno, por meio do seu Departamento de Gestão de Riscos.
9. **Diretrizes sobre como identificar, avaliar, tratar e monitorar os riscos**: o processo de gestão de riscos será desenvolvido mediante ações relativas às seguintes etapas:
   9.1. A etapa de identificação caracteriza-se na ação de reconhecer e descrever os riscos aos quais a empresa está exposta, definindo-se eventos, fontes, impactos e responsáveis por cada risco, com a participação de todos os envolvidos nos processos da empresa, nos seus diferentes níveis.
   9.2. A etapa de avaliação caracteriza-se na realização de análises qualitativas e ou quantitativas, visando à definição dos atributos de impacto e vulnerabilidade, utilizados na priorização dos riscos a serem tratados, devendo-se considerar, inclusive, o levantamento e a análise dos controles já existentes, apurando-se, assim, os riscos residuais.
   9.3. A etapa de tratamento caracteriza-se na definição do tratamento a ser dado aos riscos priorizados e como esses deverão ser monitorados e comunicados às diversas partes envolvidas, cabendo a decisão entre evitá-los; mitigá-los, pela definição de planos de ação e controles internos; compartilhá-los; ou aceitá-los.
10. A etapa de monitoramento caracteriza-se na supervisão:
    10.1. da implantação e manutenção dos planos de ação;
    10.2. da verificação do alcance das metas das ações estabelecidas, através de atividades gerenciais contínuas e ou avaliações independentes;
    10.3. da garantia de que os controles estejam sendo eficazes e eficientes;
    10.4. da detecção de mudanças no contexto externo e interno, identificando riscos emergentes;
    10.5. da análise das mudanças nos eventos de risco, tendências, sucessos e fracassos, aprendendo-se com eles.
11. **Fluxo de comunicação e consultas, internas e externas, sobre assuntos relacionados a riscos**: a comunicação dos riscos busca assegurar um fluxo tempestivo de informações relevantes relacionadas a riscos nos diversos níveis hierárquicos da CET (estratégico, tático e operacional), contemplando as etapas de identificação, avaliação (análise), tratamento e monitoramento (resposta a riscos).

11.1. A comunicação dos riscos, seja interna ou externa, é um dos resultados-chave do processo de gestão de riscos e deve ser utilizada na tomada de decisões da alta administração da empresa.

11.2. *Comunicação interna* é realizada de maneira que a Diretoria da CET transmita informações constantes (intranet, Ato do Presidente, Aviso Geral etc.) que incluam uma clara definição da filosofia e da abordagem do gerenciamento de riscos, evidenciando o seu alinhamento aos objetivos estratégicos da empresa, bem como os papeis e responsabilidades individuais ao conduzir e apoiar os integrantes da gestão baseada em riscos.

11.3. *Comunicação externa* é realizada por meio de canais de comunicação abertos (*website,* auditorias externas) cujos colaboradores (público externo) podem fornecer informações significativas referentes às exigências legais e regulatórias, de maneira pertinente e oportuna, bem como à qualidade do atendimento e ou serviço prestado pela empresa, possibilitando a sua melhoria continua.

12. **Diretrizes para a medição do desempenho da gestão de riscos**: serão estabelecidas com o objetivo de validar e revisar, periodicamente, a matriz de riscos da empresa, bem como a sua estrutura de controle interno e as ações adotadas para minimizar a ocorrência de eventos que comprometam a realização de seus objetivos.

13. **Análise crítica e aperfeiçoamento da política e das estruturas de gestão de riscos em resposta a um evento ou mudança nas circunstâncias**: será levada a efeito mediante a adoção de ações sistemáticas de avaliação e aprimoramento dos sistemas de gestão internos com o fim de prevenir a ocorrência de desvios que possam comprometer os objetivos da empresa.

13.1. A presente Política não esgota o assunto, o qual deverá ser objeto de complementação por meio de uma norma interna específica, a ser aprovada pela Diretoria.

DISPOSIÇÕES GERAIS

Vigência

14. A presente Política entrará em vigor em 30 de junho de 2018, e permanecerá vigente por prazo indeterminando.

Referências

As referências da Política são lastreadas nos princípios que regem a Administração Pública e na legislação de regência da matéria, notadamente nas disposições da Lei federal nº 6.404, de 15 de dezembro de 1976, e da Lei federal nº 13.303, de 30 de junho de 2016.

São, ainda, referência para esta Política os seguintes normativos:

Lei Federal nº 12.846/2013

Lei Orgânica do Município de São Paulo

Lei Municipal nº 8.394/1976

Lei Municipal nº 8.989/1979

Decreto Municipal nº 58.093/2018

Norma ABNT NBR ISO 31000:2009. Gestão de Riscos: Princípios e Diretrizes

Guia de Implantação de Programa de Integridade nas Empresas Estatais – Orientações para a Gestão da Integridade nas Empresas Estatais Federais. Controladoria Geral da União. Brasília, DF: 2015.

ELABORAÇÃO
Diretoria da CET

APROVAÇÃO
Conselho de Administração da CET
Em 26 de junho de 2018

DIVULGAÇÃO
Permanente