

POLÍTICA DE GERENCIAMENTO DE RISCOS

**Aprovada em 25/09/2018
Deliberação CONSAD 75.2018**

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Gestão de Riscos que tem por finalidade estabelecer os princípios, diretrizes e responsabilidades, fazendo parte de um conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua através desta declaração de intenções da Gestão de Riscos em toda a Empresa.

Art. 2º A Gestão de Riscos na Codesp auxilia na tomada de decisão proporcionando maior efetividade no atingimento de suas metas institucionais.

Art. 3º A fonte principal das definições é a Instrução Normativa Conjunta Nº 1, da Controladoria Geral da União (CGU) e do Ministério do Planejamento (MP), de 10 de maio de 2016, com adaptações para o Codesp. A saber:

I – processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

II – governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

III – objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;

IV – risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização. O risco é medido em termos de impacto e probabilidade;

V – risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

VI – risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

VII - impacto: resultado de um evento que afeta os objetivos, podendo ter efeitos positivos ou negativos e ser estimado quantitativamente ou qualitativamente;

VIII- probabilidade: medida da regularidade de ocorrência de um evento de risco num determinado período;

IX – gestão de riscos: conjunto de métodos e atividades (princípios, objetivos, estruturas, competências e processos) coordenados necessários para se gerenciar riscos eficazmente;

X – gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;

XI – auditoria interna: atividade independente e objetiva de avaliação e de consultoria. As auditorias internas no âmbito da Administração Pública se constituem na terceira linha de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos de gestão (primeira linha de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha, executada por instâncias específicas, como comitês de risco e controles internos);

XII – controle interno da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

XIII – medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados;

XIV– apetite a risco: nível de risco que uma organização está disposta a aceitar;

XV - incerteza: estado, mesmo que parcial, resultante de deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade;

XVI - matriz de riscos: instrumento gráfico no qual são demonstrados os riscos de acordo com o seu impacto, probabilidade e faixas de categorização baseadas no apetite pelo risco definidos pela Empresa;

XVII – Plano de Continuidade do Processo: É um mapa de atividades com o objetivo de tornar a execução das ações de tratamento do risco mais claras e efetivas, por meio da resposta de perguntas essenciais: O que será feito (What)? - Por que será feito (Why)? - Onde será feito (Where)? – Quando será feito (When)? - Por quem será feito (Who)? - Como será feito (How)? - Quanto vai custar (How much)?;

XVIII – accountability (responsabilidade): conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 4º A Gestão de Riscos da Codesp deve observar os seguintes princípios:

- I – agregar valor e proteger o ambiente interno da Empresa;
- II – ser parte integrante dos processos organizacionais;
- III – subsidiar a tomada de decisões;
- IV – abordar explicitamente a incerteza;
- V – ser sistemática, estruturada e oportuna;
- VI – ser baseada nas melhores informações disponíveis;
- VII – considerar fatores humanos e culturais;
- VIII – ser transparente e inclusiva;
- IX – ser dinâmica, iterativa e capaz de reagir a mudanças;
- X – apoiar a melhoria contínua dos processos na Codesp; e
- XI – estar integrada às oportunidades e à inovação.

CAPÍTULO III

DOS OBJETIVOS

Art. 5º A Gestão de Riscos tem por objetivos:

- I – aumentar a probabilidade de atingimento dos objetivos da Codesp;
- II – fomentar uma gestão proativa;
- III – atentar para a necessidade de se identificar e tratar riscos em toda a Codesp;
- IV – facilitar a identificação de oportunidades e ameaças;
- V – prezar pelas conformidades legal e normativa dos processos organizacionais;
- VI – melhorar a prestação de contas à sociedade;
- VII – melhorar a governança;
- VIII – estabelecer uma base confiável para a tomada de decisão e o planejamento;
- IX – melhorar o controle interno da gestão;
- X – alocar e utilizar eficazmente os recursos para o tratamento de riscos;
- XI – melhorar a eficácia e a eficiência operacional;
- XII – melhorar a prevenção de perdas e a gestão de incidentes;
- XIII – minimizar perdas;
- XIV – melhorar a aprendizagem organizacional; e
- XV – aumentar a capacidade da organização de se adaptar a mudanças.

Parágrafo único. A Gestão de Riscos deve estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da Codesp.

Art. 6º O Gerenciamento de Riscos deve ser implementado de forma gradual em todas as áreas da Codesp, sendo priorizados os processos organizacionais que impactam diretamente no atingimento dos objetivos definidos no seu Planejamento Estratégico.

CAPÍTULO IV

DAS DIRETRIZES

Art. 7º O processo de Gestão de Riscos compreende as atividades de maior relevância na Codesp, dispostas no Programa de Modernização e Gestão Portuária – PMGP, as quais estão em consonância com os objetivos traçados para o atingimento do seu Planejamento Estratégico. As diretrizes para o processo são definidas pelas seguintes etapas: estabelecimento do contexto, identificação, análise, avaliação, tratamento, plano de contingência, monitoramento e comunicação.

I - Estabelecimento do Contexto

Envolve a definição de diretrizes e procedimentos necessários para auxiliar no estabelecimento do Ambiente pelo Risco da Codesp e compatibilizar as demais etapas do Processo de Gestão de Riscos ao seu ambiente interno. O estabelecimento do contexto compreende duas perspectivas mutuamente complementares:

- a) **Contexto externo:** é o ambiente externo no qual a Codesp opera envolvendo fatores como: cultural, social, político, regulatório, financeiro, tecnológico, econômico, dentre outros.
- b) **Contexto interno:** é o ambiente interno no qual a Codesp opera envolvendo fatores como: governança, estrutura organizacional, funções e responsabilidades, políticas, estratégias, capacidades, competência, sistemas de informação, processos de tomada de decisão, relações com as partes interessadas, cultura organizacional, dentre outros.

II - Identificação de Riscos

O objetivo dessa etapa compreende o levantamento e organização de informações relacionadas a riscos, que possam impedir, degradar, retardar, criar, intensificar ou acelerar o cumprimento dos objetivos da Empresa. Consiste na identificação das fontes do risco, áreas de impacto, eventos (incluindo alterações nas circunstâncias) assim como suas causas (fatores de risco), consequências e impactos potenciais.

III - Análise de Riscos

Atribui a probabilidade e o impacto associado às consequências negativas, e/ou positivas, para cada evento de risco identificado, de modo a determinar os respectivos níveis de riscos.

IV - Avaliação de Riscos

Envolve avaliar o nível de risco a fim de determinar a ordem de prioridade e de que maneira e/ou com que grau de intensidade os riscos devem ser tratados.

V - Tratamento de Riscos

A etapa de tratamento de riscos é formada por um processo cíclico iniciando na apreciação dos controles existentes, na avaliação se os níveis de riscos são aceitáveis ou toleráveis, e posteriormente na análise da relação custo-benefício e de melhoria dos controles e/ou implementação de um novo tratamento para os riscos, caso seja constatado que os riscos são inaceitáveis.

As opções de tratamento, que podem ser combinadas, estão relacionadas a seguir:

- a) Mitigar o risco** - consiste em adotar medidas que reduzem o impacto e/ou probabilidade do risco para níveis considerados aceitáveis.
- b) Aceitar (tolerar) o risco** - consiste em não adotar nenhuma ação específica para modificar o risco.
- c) Transferir o risco** - consiste em transferir a responsabilidade pelo risco e/ou suas consequências para terceiros.
- d) Eliminar o risco** - consiste em interromper a atividade que dá origem ao risco, após constatar que o risco é inaceitável.

VI - Planos de Contingência

Elabora e implementa um planejamento de ações e medidas necessárias, devendo-se mantê-las prontamente disponíveis, para reduzir os impactos decorrentes da materialização de um risco.

VII – Monitoramento

É um processo cíclico de avaliação, com frequência definida para cada contexto, e consiste em acompanhar a eficácia da Gestão de Riscos na Codesp, através da análise crítica do conjunto de riscos identificados a que a Codesp está exposta e seus indicadores, da documentação e comunicação das lições aprendidas ao longo do Processo de Gestão de Riscos, a fim de diagnosticar e corrigir eventuais incompatibilidades e inadequações, favorecendo seu contínuo aperfeiçoamento.

VIII – Comunicação

Constitui fator determinante para o sucesso da Gestão de Riscos a comunicação com todas as partes interessadas ao permitir o fluxo eficaz de informações, definindo o contexto de forma apropriada com o apoio de diversas áreas de conhecimento para identificar e analisar riscos, levando em conta diferentes pontos de vista.

CAPÍTULO V

DOS INSTRUMENTOS

Art. 8º Esta política encontra sua fundamentação na legislação vigente, bem como, no que couber, em padrões, técnicas e conceitos reconhecidamente adotados pelos órgãos de controle:

- a) Instrução Normativa Conjunta CGU e Ministério do Planejamento nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;
- b) Resoluções da Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR), números 10 a 18, de 10/05/2016;
- c) Lei 12.846/2013, de 01/08/2013, que dispõe sobre a responsabilidade administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública;
- d) Decreto 8.420/2015, de 18/03/2015, que regulamenta a Lei 12.846/2013;

- e) Lei 13.303, de 30/06/2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- f) Decreto 8.945/2016, de 27/12/2016, que regulamenta a Lei 13.303/2016;
- g) Normas ABNT (Associação Brasileira de Normas Técnicas) ISO 9001:2015, 31000:2012;
- h) COSO (Committee of Sponsoring Organizations of the Treadway Commission).

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 9º O Conselho de Administração é responsável por aprovar a Política de Gestão de Riscos da Codesp e suas revisões, conforme disposto no art. 55, inciso XVII do Estatuto Social, definindo as diretrizes e estratégias a serem adotadas e determinar sua aplicação.

Art. 10 Os Diretores são responsáveis pela execução dos planos de ação de tratamento de riscos das áreas e processos sob sua supervisão.

Art. 11 A Superintendência de Desempenho, Riscos e Conformidade - SUDEC é a unidade organizacional responsável por supervisionar os sistemas de gestão de riscos.

Art. 12 A Gerência de Riscos e Controles Internos – GECOI é a responsável pela condução das ações de gerenciamento de riscos.

Art. 13 Os Gestores de processos organizacionais são responsáveis por adotar medidas de gestão de riscos, de controles internos e conformidade, e verificar continuamente sua eficácia, através de indicadores.

Art. 14 As Unidades de Gestão são responsáveis pela implementação desta política em seus segmentos de atuação, seguindo as orientações normativas emitidas sobre o tema.

Art. 15 A Auditoria Interna é responsável por aferir a efetividade do gerenciamento de riscos dos processos mapeados e suas adequações dos controles internos e conformidade.

Art. 16 O Comitê de Auditoria – COAUD é o órgão de suporte ao Conselho de Administração no que se refere ao exercício de suas funções de auditoria e de fiscalização sobre os Planos de Continuidade dos Processos e os Relatórios Periódicos de Riscos e Controles Internos.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 17 O desempenho da Gestão de Riscos será medido através dos indicadores estabelecidos no Plano de Continuidade de Processo de cada processo mapeado, na periodicidade de acordo com a ocorrência do risco.

Art. 18 Os casos omissos, exceções, bem como, os ajustes na presente Política de Gestão de Riscos devem ser submetidos à aprovação do Conselho de Administração.

Art. 19 A não observância desta política e seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regime Disciplinar e/ou no Código de Ética da Codesp.

Art. 20 Esta Política de Gestão de Riscos entra em vigor após aprovação do Conselho de Administração - CONSAD.

o O o