

POLÍTICA DE GESTÃO DE RISCOS, GOVERNANÇA E CONTROLE INTERNO DO IFES

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º – A Política de Gestão de Riscos tem por objetivo estabelecer princípios, diretrizes, governança e responsabilidades a serem observadas no processo de gestão de riscos no Instituto Federal do Espírito Santo (Ifes), de forma a possibilitar a identificação, análise, avaliação, tratamento, monitoramento, comunicação dos riscos e melhoria contínua dos processos da gestão de riscos na Reitoria e nos *campi* que integram o Ifes, incorporando a visão de riscos à tomada de decisão e contribuindo para o aprimoramento da governança institucional.

Parágrafo único. Por governança institucional entende-se como, no âmbito das organizações públicas, o conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. O processo e a estrutura de governança são baseados na gestão de riscos.

Art. 2º – A Política de Gestão de Riscos compreende as seguintes finalidades:

- I – assegurar a existência de um processo estruturado de gestão de riscos como forma de contribuição para a continuidade das atividades organizacionais e geração de valor à sociedade;
- II – contribuir para a melhoria contínua da eficiência, da eficácia e da qualidade dos serviços públicos prestados à sociedade; e
- III – racionalizar e promover a efetividade das despesas orçamentárias do Ifes.

Art. 3º – Entende-se para o fim desta Política:

- I – risco: o efeito da incerteza nos objetivos de uma organização, caracterizado esse efeito por um desvio em relação ao resultado esperado, seja positivo (oportunidade) ou negativo (ameaça);
- II – oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos;
- III – evento: um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo materializar ou não o risco;
- IV – riscos organizacionais: conjunto de riscos que permeiam todas as atividades da organização, podendo estar relacionadas ou não, e geram impacto positivo ou negativo no atingimento dos

objetivos organizacionais;

V – gestão de riscos: conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco, contribuindo para a redução da materialização de eventos que impactem negativamente seus objetivos ou para potencializar a materialização de eventos que aumentem as oportunidades de atingimento dos objetivos;

VI – tolerância ao risco: é a quantidade de risco que a organização está propensa a aceitar para alcançar seus objetivos, podendo definir ainda níveis de desvio aceitáveis durante o desempenho das suas atividades;

VII – gestor de riscos: servidor, papel exercido ou estrutura organizacional com autoridade e responsabilidade para gerenciar e tomar decisões sobre os riscos da organização;

VIII – gestor de processos: unidade organizacional, funcional ou servidor designado que detém a responsabilidade pela execução das atividades inerentes ao funcionamento organizacional ou funcional, devendo gerenciar os riscos envolvidos, porém sem poder de decisão sobre os mesmos;

IX – nível de risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos da organização; e

X – *Accountability*: responsabilidade pela prestação de contas às instâncias controladoras e à sociedade.

CAPÍTULO II

DOS PRINCÍPIOS DA GESTÃO DE RISCOS

Art. 4º – Constituem-se como princípios norteadores para a gestão de riscos no Ifes:

I – reduzir a ineficiência e o retrabalho, gerando valor à sociedade;

II - fomentar a inovação e a ação empreendedora responsáveis;

III – considerar não somente riscos, mas também as oportunidades;

IV – aplicar-se a qualquer processo de trabalho, tipo de atividade, projeto, iniciativa ou ação de plano institucional;

V – aplicar-se de forma contínua e integrada aos processos de trabalho;

VI – basear-se nas melhores informações disponíveis;

VII – ser implantada por meio de ciclos de revisão;

- VIII – contribuir para a melhoria contínua da organização;
- IX – considerar a importância dos fatores humanos e culturais; e
- X – ser dirigida, apoiada e monitorada pela alta administração.

CAPÍTULO III

DAS DIRETRIZES DO PROCESSO DE GESTÃO DE RISCOS

Art. 5º – O processo de gestão de riscos do Ifes adotará as seguintes categorizações mínimas de riscos, podendo ser ampliadas:

I – riscos estratégicos: estão associados à tomada de decisão que podem afetar negativamente o alcance dos objetivos estratégicos da organização;

II – riscos operacionais: estão associados à ocorrência de perdas (produtividade, ativos e orçamento) resultantes de falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como de eventos externos (catástrofes naturais, greves, fraudes, mudanças no contexto político e econômico etc.);

III – riscos de comunicação: estão associados a eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisão e para o cumprimento das obrigações de *accountability*;

IV – riscos de conformidade: estão associados ao não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis ao negócio, bem como de normas e procedimentos internos.

Parágrafo único. Deverão ser considerados para fins de categorização e classificação tanto os riscos internos quanto os riscos externos à organização.

Art. 6º – Como forma de racionalização das atividades e de padronização e estruturação do processo, as etapas básicas da gestão de riscos deverão compreender:

I – estabelecimento do contexto: consiste na identificação e definição dos parâmetros internos e externos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e dos critérios de riscos;

II – identificação dos riscos: consiste em buscar, reconhecer e descrever os riscos, mediante a identificação das fontes de riscos, eventos, suas causas e as consequências potenciais;

III – análise de riscos: consiste em compreender a natureza do risco e determinar o respectivo nível

de risco (severidade), mediante a combinação da probabilidade de sua ocorrência e dos possíveis impactos;

IV – avaliação dos riscos: consiste em comparar o nível de risco encontrado (severidade), durante a etapa de análise, e decidir as ações que serão tomadas para o tratamento (mitigação) e respostas (contingenciamento) aos riscos;

V – tratamento dos riscos: consiste da seleção e implementação de uma ou mais ações de tratamento para modificar o nível do risco dentro dos limites de tolerância da organização;

VI – contingenciamento dos riscos: consiste da seleção e implementação de uma ou mais ações como resposta à efetivação do evento de risco;

VII – monitoramento e análise crítica: consiste de ações de verificação, supervisão, observação crítica ou identificação da situação de risco, realizadas de forma contínua, a fim de determinar a adequação, suficiência e eficácia dos controles internos para atingir os objetivos estabelecidos; e

VIII – comunicação e consulta: consiste da manutenção de um fluxo regular e constante de informações com as partes interessadas, ocorrendo de forma concomitante durante todas as fases do processo de gestão de riscos.

§ 1º – O detalhamento das etapas enumeradas nos incisos I a VIII deste artigo, bem como os procedimentos e os instrumentos necessários ao processo de gestão de riscos, serão definidos no Manual de Gestão de Riscos, a ser estabelecido pela Diretoria de Planejamento no prazo de até 90 (noventa) dias, a partir da data de publicação desta Resolução.

§ 2º – Dada a complexidade da estrutura organizacional do Ifes, a gestão de riscos será implantada progressivamente, ou seja, as áreas iniciais para implantação serão selecionadas por meio de um comitê constituído pelo Reitor, Pró-Reitores e Diretores Gerais dos *campi*.

§ 3º – No mesmo prazo previsto no § 1º, será elaborado o Plano de Implantação da Gestão de Riscos, onde serão definidas as atividades e os prazos para a efetiva implantação da Política de Gestão de Riscos para as áreas inicialmente selecionadas no § 2º.

Art. 7º – O processo de gestão de riscos no Ifes deve observar:

I – o ambiente interno e o ambiente externo;

II – os objetivos estratégicos, táticos e operacionais;

III – a razoabilidade da relação custo-benefício nas ações para tratamento de riscos;

IV – a comunicação tempestiva sobre riscos às partes interessadas; e

V – o acompanhamento dos riscos-chave pela alta administração.

CAPÍTULO IV

DO PROCESSO DE GOVERNANÇA DA GESTÃO DE RISCOS

Art. 8º – O processo de governança da gestão de riscos será exercido pelo Comitê de Gestão de Governança, Riscos e Controle, órgão de caráter consultivo, de assessoria permanente para questões relativas à gestão de governança, riscos e controles no Instituto Federal do Espírito Santo, tendo a seguinte composição:

I – Reitor(a);

II – Pró-reitores ou seus representantes;

III – Diretores Gerais dos *campi* ou seus representantes; e

IV – Representantes que compõem o Colégio de Dirigentes.

Parágrafo único – Caberá ao Reitor(a) do Ifes, como autoridade máxima da governança da gestão de riscos, aprovar previamente e submeter ao Colégio de Dirigentes e, posteriormente, ao Conselho Superior a sua implantação, bem como quaisquer futuras revisões, e aprovar, por ato próprio, o grau de tolerância a riscos do Ifes.

Art. 9º – A governança da gestão de riscos terá a seguinte estrutura e responsabilidades:

I – Comitê de Governança, Riscos e Controles:

a) assegurar os recursos necessários, tanto no que tange ao apoio institucional quanto à estrutura aplicável ao gerenciamento de riscos, para garantir a efetiva implantação e funcionamento da Política de Gestão de Riscos;

b) institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;

c) promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;

d) promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;

e) promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;

f) aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

- g) supervisionar o mapeamento e avaliação dos riscos-chaves que podem comprometer a prestação de serviços de interesse público;
- h) liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;
- i) estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública ou atividade;
- j) aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
- k) emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos; e
- l) monitorar as recomendações e orientações deliberadas pelo Comitê.

II– Diretoria de Planejamento:

- a) elaborar a metodologia a ser utilizada para condução do processo de gestão de riscos;
- b) capacitar os gestores de riscos e processos na aplicação da metodologia e no uso de ferramentas e técnicas da gestão de riscos;
- c) promover, em conjunto com os gestores de riscos, a identificação, análise e avaliação dos riscos inerentes às atividades institucionais, levando em consideração a sua relevância e probabilidade de ocorrência;
- d) propor, em conjunto com os gestores de riscos, as ações de tratamento (mitigação) e respostas (contingenciamento) a serem adotadas para os riscos identificados, a partir dos graus de risco definidos;
- e) contribuir com a elaboração e acompanhar a execução dos planos de ação para o tratamento dos riscos;
- f) submeter ao Comitê de Governança, Riscos e Controles a proposta de grau de tolerância ao risco do Ifes para aprovação;
- g) consolidar a avaliação de riscos do Ifes, por meio da elaboração de relatórios periódicos, publicando-os em sítio institucional específico;
- h) apoiar e conscientizar os gestores sobre a importância da gestão de riscos e sobre a responsabilidade inerente a cada servidor do Ifes; e
- i) contribuir com a Auditoria Interna para a definição do escopo e abrangência dos trabalhos

relacionados a riscos.

III – Auditoria Interna:

a) avaliar o Sistema de Gestão de Riscos do Ifes, especialmente quanto aos seguintes aspectos: adequação e suficiência dos mecanismos de gestão de riscos estabelecidos, eficácia da gestão de riscos chave e conformidade das atividades executadas à política de gestão de riscos.

IV – Gestores de riscos:

a) realizar a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, à vista da dimensão dos prejuízos que possam causar;

b) propor os níveis aceitáveis de exposição ao risco, de modo a consolidar a tolerância ao risco do Ifes;

c) realizar a seleção dos riscos que deverão ser priorizados para tratamento por meio de ações de caráter imediato, a curto, médio ou longo prazos ou de aperfeiçoamento contínuo; e

d) definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e a avaliação dos resultados obtidos.

V – Gestores de processos:

a) contribuir nas atividades de identificação e avaliação dos riscos inerentes aos processos de trabalho sob sua responsabilidade ou que perpassem a sua área de atuação;

b) gerenciar os riscos inerentes aos processos de trabalho sob sua responsabilidade, de forma a mantê-los em um nível de exposição aceitável;

c) implementar os planos de ação definidos para tratamento dos riscos inerentes; e

d) comunicar ao Gestor de Riscos sobre novos riscos inerentes aos seus processos e que ainda não fazem parte da relação de riscos institucionais.

Art. 10 – São considerados gestores de riscos na Reitoria e nos *campi*, em seus respectivos âmbitos e escopos de atuação, o Reitor, os Pró-Reitores, os Diretores-Gerais e os Diretores Sistêmicos (na Reitoria e nos *campi*).

Parágrafo único – São considerados gestores de processos os servidores que sejam responsáveis pelos processos de trabalho, projetos e ações desenvolvidas nos níveis estratégicos, táticos ou operacionais no Ifes.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 11 – O processo de gestão de riscos deve ser realizado em ciclos não superiores a 4 (quatro) anos, abrangendo os processo de trabalho de todas as áreas.

Parágrafo único – O limite temporal a ser considerado para o ciclo de gestão de riscos de cada processo de trabalho será decidido pelo respectivo gestor, levando em conta o limite máximo estipulado no *caput* deste artigo.

Art. 12 – A Diretoria de Planejamento, conforme descrito no art. 9º deverá iniciar o processo para a implantação da presente Política de Gestão de Riscos no Ifes no prazo de até 120 (cento e vinte) dias, a partir da data de publicação deste Ato.

Parágrafo único – Será de dois anos o prazo para a reavaliação dos níveis de tolerância a riscos, a serem submetidos ao Reitor do Ifes, o qual compete aprová-los, conforme previsto no parágrafo único do artigo 8º.

Art. 13 – As Políticas de Segurança da Informação, Comunicação e Capacitação do Ifes deverão observar as diretrizes da Política de Gestão de Riscos no que tange ao gerenciamento de riscos e realizar suas adequações.

Art. 14 – A Política de Gestão de Riscos vincula todos os responsáveis definidos nos artigos 9º e 10 ao seu fiel cumprimento e execução, sob pena de responsabilização.

Art. 15 – Os casos omissos desta Política serão resolvidos estritamente pela Diretoria de Planejamento;

Art. 16 – Esta Política entra em vigor na data de sua publicação.

Vitória – ES, xx de xxx de 2017.