

## ANEXO ÚNICO

### POLÍTICA DE GESTÃO DE RISCOS (PGR) DA SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO (SCGE)

#### CAPÍTULO I DAS DISPOSIÇÕES GERAIS

**Art. 1º** A presente Política de Gestão de Riscos (PGR) é aplicável a todas as áreas desta Secretaria da Controladoria-Geral do Estado de Pernambuco (SCGE/PE).

**Art. 2º** Para fins desta PGR, considera-se:

I - processo: conjunto de atividades inter-relacionadas ou interativas que utilizam entradas para entregar um resultado pretendido.

II - objetivo organizacional: fim desejado que a organização pretende atingir e que orienta o seu comportamento em relação ao futuro e ao ambiente interno e externo;

III - risco: possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos;

IV - evento: ocorrência ou mudança em um conjunto específico de circunstâncias;

V - medidas de controle: medida que visa tratar as causas ou as consequências do evento de risco, de modo a fornecer segurança razoável de que os objetivos organizacionais serão alcançados, compreendendo: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas, conferências e trâmites de documentos e informações;

VI - risco inerente: nível de risco intrínseco antes da consideração das respostas que a Administração adota para reduzir a probabilidade do evento ou os seus impactos nos objetivos;

VII - risco residual: risco que ainda permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e o impacto dos riscos;

VIII - gestão de riscos: corresponde ao conjunto de ações e instrumentos que uma entidade coloca em prática para identificar e mitigar riscos relativos ao seu negócio, compreendendo, além das atividades de gerenciamento de riscos e de monitoramento, os instrumentos de governança e de gestão que suportam a concepção, a implementação, o monitoramento e a melhoria contínua da gestão de riscos.

IX - gerenciamento de riscos: processo de identificação, avaliação e resposta aos riscos, compreendendo desde as etapas de definição de contexto e escopo até a elaboração do plano de tratamento;

X - 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;

XI - controles internos: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas, conferências e trâmites de documentos e informações, estabelecidos e implementados para assegurar que as respostas aos riscos selecionados pela administração sejam executadas com eficácia.

XII - parte interessada: pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;

XIII - apetite a riscos: quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir;

XIV - tolerância a riscos: disposição da organização ou parte interessada em suportar o risco após o tratamento, a fim de atingir seus objetivos;

XV - riscos-chave: principais eventos de risco aos quais a organização está exposta e que são selecionados segundo o seu potencial de dano à materialização da estratégia do órgão e à criação de valor às partes interessadas;

XVI - gestor dos riscos: pessoa com a responsabilidade e a autoridade para coordenar o gerenciamento e realizar o monitoramento dos riscos.

**Art. 3º** Os eventos identificados durante o processo de gerenciamento de riscos da SCGE/PE deverão ser classificados de acordo com as seguintes categorias:

I - estratégico: associado à tomada de decisões avessas à missão, às metas ou ao cumprimento dos objetivos organizacionais da unidade;

II - financeiro/orçamentário: eventos que podem comprometer a capacidade da SCGE de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;

III - informacional: associado a incapacidades do órgão em salvaguardar a confidencialidade das informações de que tem a posse; disponibilizar informações para a tomada de decisões e para o cumprimento das obrigações de prestação de contas às instâncias de controle e à sociedade;

IV - imagem/Reputação: associado a eventos com o potencial de causar perdas de credibilidade da SCGE junto ao público interno e externo;

V - integridade: associado a corrupções, fraudes, irregularidades, desvios éticos ou de conduta ou improbidades, que comprometam os valores, os padrões ou os objetivos organizacionais ou afetem a gestão dos recursos e das atividades da unidade;

VI - legal: associado a alterações ou problemas na interpretação, no conhecimento ou na observância de dispositivos legais e/ou instrumentos jurídicos (inclusive jurisprudenciais), ou ainda a demandas judiciais ou administrativas, que comprometam as atividades ou os interesses da unidade ou afetem o cumprimento efetivo do ordenamento jurídico;

VII - operacional: associado a falhas, deficiências, inadequações, eventos externos, decisões judiciais ou administrativas, inseguranças ou danos, em relação a processos internos, pessoas, infraestruturas, sistemas, serviços ou produtos, que comprometam as atividades da unidade, afetem a eficácia ou a eficiência do desempenho organizacional ou ocasionem perdas;

**Art. 4º** Para fins de gerenciamento de riscos, os processos da SCGE deverão ser avaliados com base nos seguintes critérios:

- I. relevância estratégica: relevância para a realização dos objetivos-chave da organização, cujo peso é 3.
- II. imagem institucional: percepção da imagem da SCGE perante o Governo, os órgãos e entidades estaduais e a Sociedade, cujo peso é 2; e
- III. maturidade: prática de gestão consistente e padronizada, cujo peso é 1.

**§1º** Serão objeto do gerenciamento de riscos a proporção de 20% dos processos com a maior pontuação resultante da aplicação dos critérios.

**§2º** Desde que formalmente justificado, o dirigente máximo poderá retirar ou incluir processo(s) da planilha de priorização.

**Art. 5º** A SCGE deverá elaborar, antes da realização do gerenciamento de riscos, a Declaração de Appetite a Riscos, que consiste no documento técnico aprovado pelo Conselho Deliberativo de Gestão (CDG) que define o posicionamento institucional acerca do seu apetite a risco, trazendo, no mínimo, as seguintes informações.

I - a missão da organização;

II - categorias e níveis de risco definidos pelo órgão;

III - apetite a risco em função do nível de riscos e de outros critérios estabelecidos pela gestão;

IV - opções de tratamento por tipo de risco; e

V - unidades administrativas responsáveis por sua aprovação, revisão e monitoramento;

§1º O corpo administrativo da SCGE/PE deverá considerar o apetite a risco na elaboração de sua estratégia, na fixação de seus objetivos e na implementação de novas medidas de controles internos.

§2º A Declaração de Apetite a Riscos da SCGE-PE deverá ser reexaminada a cada quatro anos, na elaboração do planejamento estratégico do órgão, ou sempre que houver mudanças significativas nos ambientes interno e externo que legitimem a sua alteração.

**Art. 6º** A SCGE deverá elaborar Plano de Comunicação com o objetivo de garantir que as partes interessadas no processo de gestão de riscos tenham informações e possam supervisionar e tomar as decisões de forma eficiente, contendo, no mínimo, as seguintes informações:

I - produto;

II - objetivo do produto/entrega;

III - emissor;

IV - receptor;

V - frequência;

VI - meio de comunicação; e

VII - sistema a ser utilizado para envio da comunicação.

Parágrafo único. O plano de comunicação poderá também prever um conjunto de medidas necessárias para fomentar o conhecimento dos colaboradores em relação aos seguintes temas:

- a) promoção da conscientização e do entendimento da gestão de riscos através de informações sobre o que é, qual o seu objetivo, os benefícios e a quem se destina; e
- b) disseminação de informações relevantes sobre o plano de Gestão de Riscos, comunicando sobre as atividades e os seus resultados.

**Art 7º** A SCGE deverá elaborar Plano de Monitoramento e Melhoria Contínua, estabelecido com o objetivo de propor instrumentos e ações que possibilitem o acompanhamento e o aperfeiçoamento da gestão de riscos, sendo constituído, no mínimo, pelas seguintes informações:

I - ações propostas de monitoramento e de melhoria contínua;

II - modelo de planilha de monitoramento;

III - previsão da utilização de Indicadores de desempenho, nos casos em que for possível o cálculo; e

IV - periodicidade do monitoramento.

## **CAPÍTULO II DOS PRINCÍPIOS E DOS OBJETIVOS**

**Art. 8º** A Gestão de Riscos da SCGE/PE deverá observar as seguintes diretrizes principiológicas:

- I - criar, proteger e agregar valores institucionais;
- II - ser parte integrante dos processos organizacionais de maneira contínua;
- 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, contextos internos e externos e perfil de risco da instituição;
- VIII - ser transparente e inclusiva;
- IX - ser dinâmica, interativa e capaz de reagir a mudanças;
- X - apoiar e facilitar a melhoria contínua da instituição;
- XI - estar integrada às oportunidades e à inovação;
- XII - ser personalizada diante das necessidades do órgão;
- XIII - ser implantada por meio de ciclos de revisão;
- XIV - ser dirigida, apoiada e monitorada pela alta administração; e
- XV - manter a razoabilidade da relação custo-benefício nas ações para tratamento de riscos.

**Art. 9º** A Gestão de Riscos da SCGE/PE promoverá pelo menos estes objetivos:

- I - auxiliar e fortalecer o planejamento e a tomada de decisão, em base confiável, com vistas a prover razoável segurança no cumprimento da missão e da visão e no alcance dos objetivos organizacionais;
- II - capacitar a organização à gestão proativa e à adaptação a mudanças;
- III - identificar e tratar eventos de riscos, em toda a instituição, que afetem a consecução dos objetivos organizacionais;
- IV - facilitar a identificação de oportunidades e ameaças;
- V - prezar pela conformidade normativa dos processos organizacionais;
- VI - otimizar a prestação de contas à sociedade;
- VII - aperfeiçoar a governança;
- VIII - aprimorar os controles internos da gestão;
- IX - utilizar e alocar os recursos para o tratamento de eventos de riscos;
- X - fomentar a eficácia e a eficiência da instituição;
- XI - prevenir e minimizar perdas e gerir incidentes; e
- XII - incentivar a aprendizagem organizacional.

### **CAPÍTULO III**

#### **DOS PROCEDIMENTOS, DAS RESPONSABILIDADES E DAS COMPETÊNCIAS**

**Art. 10.** A Gestão de Riscos deverá ser implementada de forma gradual em todas as áreas da SCGE/PE, por priorização de processos institucionais, no que couber, a partir dos critérios de relevância estratégica, imagem institucional e maturidade do processo.

**Art. 11.** A operacionalização do Gerenciamento de Riscos deverá ser descrita através de um **guia metodológico**, que deverá contemplar, no mínimo, as seguintes etapas:

- I - definição de contexto e escopo: informações básicas da instituição, para definir a condução da Gestão de Riscos, tais como: informações sobre a Unidade Gestora; descrição resumida do escopo; processos escolhidos; responsáveis pela condução do gerenciamento de riscos; e análise dos contextos interno e externo.
- II - identificação de eventos de riscos: processo de detecção e descrição dos eventos de riscos e demais elementos associados;

- III - identificação e avaliação dos controles existentes: verificação e análise dos controles internos preexistentes;
- IV - cálculo do risco residual: apreciação detalhada dos eventos de riscos, suas probabilidades e impactos, considerando a influência das medidas de controle existentes e a sua eficácia;
- V - validação do risco inerente: consolidação do risco intrínseco do evento de risco concretizado, sem as medidas dos controles internos preexistentes;
- VI - definição de medidas de controles internos: regra geral do grau de resposta aos eventos de riscos; e
- VII - elaboração do plano de tratamento: elaboração de proposta de controles, por meio da definição de atividades, planos, métodos, indicadores e procedimentos interligados para tratar a causa e/ou a consequência do evento de risco.

Parágrafo Único. Durante todo o procedimento de Gestão de Riscos deve haver integração e compartilhamento com todas as partes interessadas, bem como monitoramento contínuo, com vistas à melhoria.

**Art. 12.** São partes interessadas do processo de Gerenciamento de Riscos:

- I - Conselho Deliberativo de Gestão – CDG;
- II - Assessoria Especial de Controle Interno – AECI; e
- III - Colaboradores da Secretaria da Controladoria-Geral do Estado de Pernambuco.

**Art. 13.** No âmbito do procedimento de Gestão de Riscos da SCGE/PE, compete ao Conselho Deliberativo de Gestão - CDG, instituído pelo Decreto nº 49.993, de 18 de dezembro de 2020, que alterou o art. 3º do Anexo I do Decreto Estadual nº 47.667, de 1º de Julho de 2019, cujo Regimento Interno foi aprovado pela Portaria SCGE nº 45, de 21 de dezembro de 2020:

- I - direcionar o estabelecimento, a manutenção, o monitoramento e o aprimoramento da Gestão de Riscos e dos Controles Internos, nos termos do art. 17 do Decreto nº 46.855, de 07 de dezembro de 2018;
- II - promover ampla discussão sobre as iniciativas estratégicas relacionadas à Gestão de Riscos e as ações para sua implementação;
- III - acompanhar e propor ações para elaboração, implementação, monitoramento, avaliação e revisão dos instrumentos de Gestão de Riscos, definindo periodicidade de cada ciclo e os responsáveis;
- IV - incentivar e promover iniciativas que busquem implementar o acompanhamento de resultados da Gestão de Riscos, fomentando soluções para melhoria do desempenho institucional com base em indicadores e demais instrumentos para o aprimoramento do processo decisório;
- V – instituir grupos de trabalho para a produção de estudos, análises e opinativos sobre o processo de gerenciamento de riscos;
- VI - criar Comissão de Gestão de Riscos para auxiliar a AECI em suas atribuições, quando necessário;
- VII - incentivar o alinhamento da Gestão de Riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade da instituição, nos moldes dos Decretos Estaduais nº 40.271, de 9 de Janeiro de 2014, e nº 46.855, de 07 de dezembro de 2018;
- VIII - dirimir eventuais conflitos de atuação decorrentes do processo de Gerenciamento de Riscos.
- IX - apoiar institucionalmente a Gestão de Riscos no órgão, por meio da disponibilização de recursos, da promoção do relacionamento tempestivo entre as partes interessadas e do desenvolvimento contínuo dos colaboradores;
- X - validar a metodologia de Gestão de Riscos e suas revisões;

- XI - definir o nível de risco que o órgão está disposto a aceitar enquanto persegue seus objetivos através da Declaração de Appetite;
- XII - aprovar os Planos de Tratamento elaborados com as medidas de controle interno necessárias para a mitigação dos principais riscos encontrados nos processos organizacionais do órgão;
- XIII - aprovar a Política de Gestão de Riscos da SCGE;
- XIV - aprovar a Declaração de Appetite a Riscos da SCGE e suas revisões;
- XV - validar o rol de processos priorizados para os ciclos de gerenciamento de riscos do órgão;
- XVI - aprovar os critérios de seleção dos riscos-chave propostos pela AECI;
- XVII - monitorar, a partir de reportes periódicos elaborados pela AECI, os riscos-chave do órgão;
- XVIII - supervisionar a atuação das demais instâncias da Gestão de Riscos;
- XIX - aprovar o Plano de Comunicação da Gestão de Riscos.

**Art. 14.** No âmbito da PGR, compete à Assessoria Especial de Controle Interno – AECI de que trata o inciso VI do art. 4º do Decreto Estadual nº 47.667, de 1º de Julho de 2019:

- I - auxiliar o CDG no processo de Gestão de Riscos, nos termos do art. 8º desta Política, considerando os contextos externo e interno;
- II - elaborar a metodologia de Gerenciamento de Riscos e suas revisões;
- III - consolidar, antes do término de cada ciclo, os resultados do Gerenciamento de Riscos das diversas áreas da instituição em relatório gerencial e encaminhá-lo ao CDG;
- IV - requisitar aos responsáveis pela Gestão de Riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração do relatório gerencial;
- V - sugerir capacitações na temática de Gestão de Riscos para os colaboradores da instituição;
- VI - elaborar Plano de Comunicação de Gestão de Riscos;
- VII - elaborar a Declaração de Appetite a Riscos do órgão e suas revisões;
- VIII - elaborar a Política de Gestão de Riscos do órgão e suas revisões;
- IX - validar os indicadores gerenciais de acompanhamento definidos pela primeira linha responsável pela gestão de riscos do órgão;
- X - coordenar os ciclos de gerenciamento de riscos no órgão;
- XI - propor os processos que farão parte do escopo dos ciclos de gerenciamento de riscos do órgão;
- XII - supervisionar o monitoramento operacional realizado pelo Gestor dos Riscos;
- XIII - pactuar com o gestor dos riscos a periodicidade de atualização do status das medidas de controle dispostas nos Planos de Tratamento e dos indicadores;
- XIV - propor critérios para a seleção dos riscos-chave do órgão; e
- XV - comunicar tempestivamente ao CDG a evolução dos níveis de riscos e a efetividade das medidas de controles internos implementadas para contrapor os riscos-chave da SCGE.

**Art. 15.** Compete aos demais colaboradores responsáveis pela Gestão de Riscos dos processos organizacionais da SCGE/PE:

- I - avaliar os contextos interno e externo dos processos priorizados em cada ciclo de gerenciamento de riscos;
- II - identificar, classificar, analisar e avaliar os eventos de riscos dos processos sob sua responsabilidade;
- III - identificar e avaliar controles internos existentes associados aos eventos de risco identificados;

IV - apreciar os eventos de riscos, segundo a probabilidade de ocorrência e o impacto da materialização, considerando a influência das medidas de controle existentes e a sua eficácia;

V - eleger os riscos-chave do processo, dentre aqueles identificados previamente;

VI - elaborar planos de tratamento com o objetivo de detalhar a implementação das medidas de controle selecionadas, de modo que os arranjos sejam compreendidos, e o progresso das ações monitorado

VII - implementar as medidas de controles internos dispostas nos planos de tratamento nos processos organizacionais sob sua responsabilidade;

VIII - revisar os planos de tratamento, quando cabível, em obediência ao disposto no guia metodológico;

IX - estabelecer indicadores gerenciais de acompanhamento da implementação das medidas de controle interno previstas no Plano de Tratamento;

X - monitorar a implementação dos controles propostos e manter atualizada a Planilha de Monitoramento;

XI - detalhar o custo presumido das medidas de controle, bem como o benefício financeiro esperado, quando cabível;

XII - informar sobre mudanças significativas nos processos organizacionais sob sua responsabilidade; e

XIII - comunicar à AECI a evolução dos níveis de riscos e a efetividade das medidas de controles internos implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

Parágrafo único. Cabe ao Diretor ou cargo equivalente indicar o gestor dos riscos dos processos a ele vinculados com base, preferencialmente, nos requisitos objetivos listados a seguir:

a) tenham conhecimento sobre a metodologia de Gerenciamento de Riscos definida para o órgão;

b) estejam familiarizados com o processo organizacional objeto do ciclo de Gerenciamento de Riscos; e

c) tenham participado das etapas de identificação, análise e avaliação dos principais riscos do processo a que estejam vinculados.

#### **CAPÍTULO IV DAS DISPOSIÇÕES FINAIS**

**Art. 16.** Esta PGR será revista a cada 02 (dois) anos ou sempre que necessário, a partir de proposta do CDG, no intuito de mantê-la atualizada diante de mudanças no ambiente interno ou externo.

**Art. 18.** Fica o CDG autorizado a deliberar sobre os atos necessários à regulamentação desta Política e decidir sobre os casos omissos.

**Art. 19.** O CDG, a Assessoria Especial de Controle Interno e os demais colaboradores responsáveis pela Gestão de Riscos dos processos organizacionais deverão manter fluxo regular e constante de informações entre si.

**Art. 20.** Fica autorizada a existência de outras políticas de gestão de riscos relacionadas a temas específicos desde que não conflitem com as diretrizes gerais dispostas neste Anexo Único.