PORTARIA Nº , DE DE DE 2022.

Dispõe sobre a Política de Gestão de Riscos da NOME DA PASTA e dá outras providências.

O(A) Secretário/Presidente do(a) (nome da pasta), no uso de suas atribuições que lhes conferem o inciso III, do art. 56 da Lei nº 20.491/19, e

Considerando o Programa de *Compliance* Público por meio da Implantação da Gestão de Riscos Corporativos, com base nas Boas Práticas de Governança Corporativa,o qual é gerido pela Controladoria-Geral do Estado de Goiás - CGE;

Considerando o modelo *Committee of Sponsoring Organizations of the Treadway Commission* - COSO 2013 e atualizações – *Internal Control – Integrated Framework* (ICIF);

Considerando o COSO ERM 2017 - Gerenciamento de Riscos Corporativos - Integrado com a Estratégia e Desempenho;

Considerando a Norma ABNT NBR ISO 31000:2018 que estabelece princípios e diretrizes para a implantação da Gestão de Riscos;

Considerando a Norma ABNT NBR IEC (ISO) 31010:2021 que fornece orientações sobre a seleção e aplicação de técnicas para o processo de avaliação de riscos em uma ampla gama de situações.

Considerando a Norma ABNT ISO 37.301/2021 - Sistema de Gestão de Compliance;

Considerando a iniciativa estratégica de Implantação do Eixo IV do Programa de Compliance Público, que trata da Gestão de Riscos nos entes da Administração Direta e Indireta do Poder Executivo do Estado de Goiás, instituído pelo Decreto Estadual nº 9.406/19; e

Considerando, ainda, os modelos de boas práticas gerenciais em Gestão de Riscos e Controle Interno a serem adotados no âmbito da Administração Pública do Estado de Goiás, estabelecidos no art. 8º do Decreto acima citado, em busca de se evoluir em maturidade da prática,

RESOLVE:

DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir a Política de Gestão de Riscos no âmbito do(a) (nome da pasta), que compreende:

I – o objetivo;
II – os princípios;
III – as diretrizes;
IV – as responsabilidades;
V – o processo de gestão de riscos.

Art. 2º A Política de Gestão de Riscos tem como premissa básica o alinhamento ao Planejamento Estratégico do (nome da pasta), bem como aos objetivos estratégicos do órgão/instituição, com vistas a garantir os valores fundamentais das organizações em consonância com as Cadeias de Valores devidamente definidas por cada instituição.

DO OBJETIVO

Art. 3º A Política de Gestão de Riscos tem por objetivo estabelecer os princípios, as diretrizes, as responsabilidades e o processo de gestão de riscos no(a) (nome da pasta), com vistas à análise de riscos no processo de tomada de decisão, em conformidade com as boas práticas de governança adotadas no setor público.

Parágrafo único. A Política definida nesta Portaria deverá ser observada por todas as áreas e níveis de atuação do(a) (nome da pasta), sendo aplicável a seus respectivos processos de trabalho, projetos, atividades e ações.

Art. 4º A Política de Gestão de Riscos promoverá:

I – a identificação de eventos em potencial que afetem a consecução dos objetivos institucionais;
II – o alinhamento do apetite ao risco com as estratégias adotadas;
III – o fortalecimento das decisões em resposta aos riscos;
IV – o aprimoramento dos controles internos administrativos;
V - a integração da gestão de riscos aos objetivos e processos organizacionais;
VI - a tomada de decisões baseada em riscos.

DOS PRINCÍPIOS DE GESTÃO DE RISCOS

Art. 5º A gestão de riscos observará os seguintes princípios, na sua busca por criação e proteção de valor:

I – ser parte integrante de todas as atividades organizacionais;
II – ser estruturada e abrangente;
III – ser personalizada e proporcional aos contextos externo e interno da organização;
IV – ser inclusiva;
V – ser baseada nas melhores informações disponíveis;
VI – considerar fatores humanos e culturais;
VII – ser dinâmica, iterativa e capaz de reagir a mudanças;
VIII - garantir a manutenção dos valores da organização;

IX – favorecer a melhoria contínua na organização.

DAS DIRETRIZES DE GESTÃO DE RISCOS

Art. 6º Para fins desta Portaria considera-se:

I –Apetite pelo risco – quantidade e tipo de riscos que uma organização está disposta a aceitar na busca para atingir seus objetivos estratégicos e operacionais;

II - Atitude perante o risco – abordagem da organização para analisar e avaliar o risco e, com isso, decidir reduzir, evitar, compartilhar ou aceitá-lo;

III - Auditoria Baseada em Riscos (ABR): atividade utilizadora de metodologia que associa a auditoria interna ao arcabouço global das práticas adotadas para a consecução da gestão de riscos em uma organização, possibilitando que a mesma dê razoável garantia à alta gestão dos órgãos e das entidades de que os riscos estão sendo gerenciados de maneira eficaz em relação ao apetite por riscos;

IV - Aversão ao risco – atitude de afastar-se de riscos;

V - Consequência – resultado de um evento que afeta os objetivos da unidade ou mesmo da organização, após materialização do risco;

VI - Controle – medida que visa mitigar ou reduzir o nível do risco;

VII - Critérios de risco – termos de referência para avaliar a significância do risco e para apoiar os processos de tomada de decisão;

VIII - Estrutura de gestão de riscos – conjunto de elementos que fornecem os fundamentos e disposições organizacionais para, metodologicamente, conceber, implementar, monitorar, rever e melhorar continuamente a gestão do risco em toda a organização;

IX - Evento – ocorrência ou alteração em um conjunto específico de circunstâncias;

X - Fonte de risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para materializar o risco;

XI - Gestão de riscos – atividades coordenadas metodologicamente para dirigir e controlar uma organização, no que diz respeito ao risco;

XII - Impacto – efeito resultante da ocorrência do evento, para a organização;

XIII - Nível de risco – magnitude de um risco expressa na combinação da consequência (impacto) e de sua probabilidade de ocorrência;

XIV - Parte interessada – pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;

XV - Perfil de risco – descrição de um conjunto qualquer de riscos, sendo que o conjunto de riscos pode conter riscos que dizem respeito a toda a organização ou a parte da organização;

XVI - Plano de gestão de riscos – plano dentro de uma estrutura de gestão de riscos, especificando a abordagem, os componentes de gestão (procedimentos, práticas, atribuição de responsabilidades, sequência e cronograma das atividades) e os recursos a serem aplicados para gerenciar riscos;

XVII - Política de gestão de risco – declaração das intenções, princípios, diretrizes e responsabilidades de uma organização relacionadas ao processo de gestão de riscos;

XVIII - Probabilidade – chance de algo acontecer;

XIX - Processo de avaliação de riscos – processo global de identificação de riscos, análise de riscos e avaliação de riscos;

XX - Processo de gestão de riscos – aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos;

XXI - Proprietário do risco – pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;

XXII - Riscos – efeito da incerteza nos objetivos organizacionais;

XXIII - Riscos-chave – são aqueles que podem afetar significativamente o alcance dos objetivos e o cumprimento da missão institucional, a imagem e a segurança da organização e de pessoas. Devido ao impacto potencial nos resultados da organização, os riscos-chave devem ser monitorados diretamente pelo Comitê Setorial;

XXIV - Risco inerente – risco ao qual se expõe face à inexistência de controles que alterem o impacto ou a probabilidade do evento;

XXV - Risco residual – risco remanescente após a implantação dos controles adicionais e/ou ajustes dos controles existentes para o tratamento do risco;

XXVI - Tolerância ao risco – é a disposição da organização em suportar o risco após a implantação do tratamento.

Art. 7º A Política de Gestão de Riscos abrange as seguintes categorias de riscos (a pasta poderá definir quais categorias de riscos irá utilizar):

I – Estratégicos – riscos que causam impactos sobre os objetivos estratégicos e a execução da estratégia planejada;

II – De Conformidade – riscos que se referem ao não atendimento das normas legais vigentes;

III – Financeiros – riscos que se relacionam à inadequada gestão de caixa ou aplicação de recursos;

IV – Operacionais – riscos que prejudicam a execução ou o progresso dos processos internos;

V – Ambientais – riscos que causam impacto no meio ambientes;

VI – De Tecnologia da Informação – riscos que se referem à indisponibilidade ou inoperância de equipamentos e sistemas informatizados;

VII – De Recursos Humanos – riscos decorrentes da incapacidade em gerir recursos humanos;

VIII - Combate à Corrupção - riscos relacionados à fraude e à corrupção em qualquer uma das categorias acima.

Art. 8º São elementos estruturantes da Gestão de Riscos do(a) (nome da pasta) a Política de Gestão de Riscos, o Comitê Setorial de Compliance Público, a Secretaria Executiva de Compliance, o Processo de Gestão de Riscos e as Ações de Controle.

DAS RESPONSABILIDADES PELA GESTÃO DE RISCOS

Art. 9º São considerados proprietários dos riscos, em seus respectivos âmbitos e escopos de atuação, os responsáveis pelos processos de trabalho, projetos, atividades e

ações desenvolvidas nos níveis estratégicos, táticos ou operacionais da do(a) (nome da pasta).

Art. 10. Compete aos proprietários dos riscos, relativamente aos processos de trabalho e iniciativas sob sua responsabilidade:

I - identificar, analisar e avaliar os riscos dos processos, atividades e projetos sob sua responsabilidade;

II - identificar e implantar controles preventivos e corretivos;

III - registrar como são feitas as ações de controle existentes (aquelas que eram executadas antes do risco ser identificado);

IV - elaborar um plano de ação para as ações de controle a implantar sob sua responsabilidade;

V - registrar e monitorar todos os eventos relacionados aos riscos sob sua responsabilidade, inclusive os indicadores de monitoramento;

VI - apresentar os relatórios gerenciais (mínimo quadrimestralmente) dos riscos, acima do apetite a risco da organização, ao Comitê Setorial;

VII - monitorar se os controles implantados para mitigar os riscos são suficientes e adequados para manter o(s) risco(s) dentro do apetite a risco da instituição;

VIII - realizar a análise crítica do gerenciamento dos riscos sob sua responsabilidade, reportando à Secretaria Executiva e/ou ao Comitê Setorial as alterações que precisam ser efetivadas, com vistas à melhoria contínua do processo e a redução do nível do risco, sempre que possível;

IX - estimular e favorecer a equipe a se capacitar em gestão de riscos para que ela seja envolvida em todas as etapas da gestão de riscos, inclusive nas decisões quanto ao tratamento dos riscos.

Art. 11. Compete à Secretaria Executiva de *Compliance* ou equivalente:

I – orientar e monitorar funções e responsabilidades pela gestão de riscos em todas as áreas da organização, especialmente no preenchimento dos Relatórios de Gerenciamento de Riscos no Sistema Smartsheet pelos proprietários dos riscos;

II – coordenar a revisão periódica do processo de gestão de riscos com vistas a sua melhoria contínua;

III – coordenar e monitorar a implantação da gestão de riscos em novas áreas e/ou projetos, até que esteja consolidada em toda a organização;

IV – monitorar as ações que estão em realização para evolução da maturidade em Gestão de Riscos;

V – atuar na interlocução entre o Comitê Setorial e os proprietários de riscos e/ou responsáveis pela implantação e execução de ações de controle;

VI – comunicar ao Comitê Setorial o andamento do gerenciamento de riscos em todas as áreas, por toda a organização;

VII – auxiliar no agendamento e pauta das reuniões do Comitê Setorial;

VIII – atuar na disseminação e na internalização da cultura de Gestão de Riscos, por meio de reuniões, palestras, oficinas, dentre outros eventos;

IX – promover a interlocução com a CGE, visando o atendimento das recomendações emitidas relacionadas ao processo de gestão de riscos;

X – auxiliar o Comitê Setorial no monitoramento e no atendimento às recomendações emitidas pela Câmara de Compliance;

XI – estimular a capacitação continuada dos servidores em cursos afetos à gestão de riscos, especialmente naqueles ofertados pela Escola de Governo;

XII – coordenar o trâmite de documentos relevantes afetos da gestão de riscos, preferencialmente em unidade própria no Sistema Eletrônico de Informações (SEI);

XIII – acompanhar e monitorar a implementação das ações dos eixos I a III do Programa de Compliance Público, especialmente quanto ao cumprimento dos quesitos definidos no ranking do PCP.

Art. 12. Compete à Assessoria de Controle Interno (quando houver este cargo na pasta), no que se refere à gestão de riscos:

I – assessorar o Secretário/Presidente, sob a orientação da Controladoria-Geral do Estado, na implantação do Programa de Compliance Público do Estado de Goiás;

II – realizar a interlocução da pasta com Controladoria-Geral do Estado;

III - orientar a elaboração do plano de ação anual para a expansão da gestão de riscos em conjunto com a Secretaria Executiva de *Compliance*;

IV - orientar a elaboração do plano de ação para a evolução da maturidade em gestão de riscos da pasta;

V - facilitar, assessorar e treinar os membros Secretaria Executiva para o exercício regular das suas atribuições;

VI – apoiar as ações de capacitação e os eventos nas áreas relacionadas ao Programa de Compliance Público do Estado de Goiás;

VII - realizar a atividade de auditoria interna, demandada pela CGE, associada à estratégia e prioridades da pasta, com foco nos objetivos, metas, riscos associados e em como esses riscos são gerenciados.

Art. 13. Compete ao Comitê Setorial de Compliance Público:

I – fomentar as práticas de Gestão de Riscos;

II - definir o escopo da gestão de riscos;

III – indicar os proprietários de riscos;

IV - designar os servidores que comporão a Secretaria Executiva;

V – acompanhar de forma sistemática e periódica a gestão de riscos do escopo delineado, com o objetivo de garantir a sua eficácia e o cumprimento de seus objetivos;

VI - realizar a análise crítica e promover melhorias no processo de gestão de riscos;

VII - aprovar o plano de ação anual para a expansão da gestão de riscos;

VIII – definir, monitorar, comunicar e revisar o apetite e a tolerância a riscos da pasta;

IX - aprovar os riscos que deverão ser tolerados acima do apetite a risco da instituição;

X – monitorar o cumprimento da Política de Gestão de Riscos;

XI – revisar a política de gestão de riscos;

XII– monitorar os indicadores-chaves dos riscos estratégicos;

XIII – estimular a cultura de Gestão de Riscos;

XIV – acompanhar o cumprimento de suas decisões;

XV – definir, acompanhar e revisar o nível o nível de maturidade em gestão de riscos almejado da instituição;

XVI – acompanhar a implementação das ações dos eixos I a III do Programa de Compliance Público;

XVII - assegurar que a gestão de riscos esteja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos estratégicos da organização;

XVIII - revisar periodicamente os riscos identificados da instituição acima do apetite a riscos, visando fornecer direção clara sobre o gerenciamento de riscos;

XIX - estabelecer parcerias com outras instituições para reduzir os riscos compartilhados.

DO PROCESSO DE GESTÃO DE RISCOS

Art. 14. Serão adotados como referências técnicas para a gestão de riscos as normas ABNT NBR ISO 31000:2018 e ABNT NBR ISO 31010:2021, agregadas ao COSO 2013 - Controles Internos – Estrutura Integrada e COSO ERM 2017 - Gerenciamento de Riscos Corporativos - Integrado com a Estratégia e Desempenho compreendido pelas seguintes fases:

I – Comunicação e Consulta – processos contínuos e interativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos;

II – Estabelecimento do Escopo – definição do direcionamento das atividades de gestão de riscos, níveis considerados e alinhamento aos objetivos;

III - Estabelecimento do Contexto – definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos;

IV - Estabelecimento de Critérios de Risco – especificação da quantidade e tipo de risco que a organização pode ou não assumir em relação aos objetivos, bem como estabelecimento de critérios para avaliar a significância do risco e apoiar no processo decisório;

V – Identificação dos Riscos – busca, reconhecimento e descrição dos riscos, mediante a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais;

VI – Análise dos Riscos – compreensão da natureza do risco e à determinação do seu respectivo nível mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis;

VII – Avaliação dos Riscos – processo de comparação dos resultados da análise de risco com os critérios do risco para determinar se o risco e/ou sua respectiva magnitude é aceitável ou tolerável, auxiliando na decisão sobre o tratamento dos riscos;

VIII – Tratamento dos Riscos – processo para modificar o risco, envolvendo a seleção da(s) opção(ões) mais apropriada(s) de tratamento, incluindo o balanceamento de benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação, podendo ocorrer dentre as seguintes estratégias de respostas aos riscos, podendo envolver as ações de evitar, aceitar, reduzir e compartilhar;

IX – Estabelecimento de Controles – implantação de ações de controle que visam reduzir a probabilidade de materialização do risco e/ou seus efeitos, diminuindo a exposição das atividades aos riscos;

X – Monitoramento e Análise Crítica – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado, sendo que mudanças significativas nos riscos gerenciados deverão ser reportadas, a qualquer tempo, ao Comitê Setorial;

XI - Registro e Relato – processo de documentação, por meio de mecanismos apropriados, da gestão de riscos e de seus resultados, sendo parte integrante da governança da organização, melhorando a qualidade do diálogo com as partes interessadas e apoiando a Alta Direção e os órgãos de supervisão a cumprirem suas responsabilidades.

§1º Eventuais conflitos de atuação decorrentes do processo de gestão de riscos serão dirimidos pelo Comitê Setorial de Compliance Público.

§2º A gestão de riscos deverá fazer parte de todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações.

Art. 15. A elaboração de um Plano de Ação para a expansão da Gestão de Riscos deverá ser feita no início de cada exercício, com vistas a definir/atualizar o escopo das áreas ou processos a serem mapeados no exercício até a completa implantação da gestão de riscos em toda a pasta. Esse Plano deverá compreender as fases previstas no art. 14 desta Portaria.

Art. 16. O processo de gestão de riscos deve ser objeto de revisão periódica, sempre que necessário, com prazo não superior a 1 (um) ano, abrangendo as áreas ou processos em que a gestão de riscos já foi implantada do(a) (nome da pasta).

Parágrafo único. O limite temporal a ser considerado para o ciclo de gestão de riscos de cada processo de trabalho será decidido pelo respectivo proprietário do risco e reportado ao Comitê Setorial, levando em consideração o limite máximo estipulado no *caput*.

DAS DISPOSIÇÕES GERAIS

Art. 17. A(O) (nome da pasta) manterá registro formal de todos os atos administrativos provenientes do programa de Compliance Público (PCP) a fim de fornecimento de dados para revisão periódica interna e para a consultoria e auditoria baseada em riscos da Controladoria Geral do Estado.

Art. 18. A(O) (nome da pasta) estabelecerá plano de comunicação entre as partes interessadas internas e externas.

Art. 19. Os proprietários dos riscos a que se refere o art. 10 desta Portaria deverão implantar a presente política de gestão de riscos a partir da data de publicação desta Portaria.

Art. 20. Durante a realização da primeira Auditoria Baseada em Riscos – ABR, o Comitê Setorial de Compliance Público do(a) (nome da pasta) deverá definir os seus níveis toleráveis de riscos.

Art. 21. Os casos omissos ou excepcionais serão resolvidos pelo Comitê Setorial de Compliance Público de acordo com as orientações a serem emanadas da CGE.

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

Nome do Secretário/Presidente
Secretário/ Presidente do(a) (nome da pasta)