DECRETO Nº 289/2026, DE 27 DE MAIO DE 2026

Institui a Política de Gestão de Riscos do Programa de Compliance Público Municipal no município de Santa Bárbara de Goiás e dá outras providências.

Eu Job Martins de Deus, PREFEITO DO MUNICÍPIO DE SANTA BÁRBARA DE GOIÁS, no uso de suas atribuições legais; e

CONSIDERANDO o Programa de *Compliance* Público Municipal por meio da implantação da gestão de riscos, com base nas Boas Práticas de Governança;

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

CONSIDERANDO a iniciativa estratégica para a implantação do Eixo I - Governança do Programa de *Compliance* Público Municipal, nos entes do Poder Executivo do Município de *Santa Bárbara de Goiás* , instituído pelo Decreto Municipal nº 288/2026;

DECRETA:

CAPÍTULO I

Disposições Gerais

Art. 1º Este Decreto institui a política de gestão de riscos no âmbito municipal que compreende:

I - o objetivo;

II - os princípios;

III - as diretrizes;

IV - as responsabilidades; e

V - o processo de gestão de riscos.

Art. 2º A política de gestão de riscos tem como premissa o alinhamento ao Planejamento Estratégico do Município.

CAPÍTULO II

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 município, com vistas

à incorporação da análise de riscos à tomada de decisão, em conformidade com as boas práticas de governança adotadas no setor público.

Parágrafo único. A Política definida nessa portaria deverá ser observada pelas áreas que contemplem a execução e monitoramento de riscos, sendo aplicável a seus respectivos processos.

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.

CAPÍTULO III

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 - facilitar a melhoria contínua da organização.

CAPÍTULO IV

Das Diretrizes de Gestão de Riscos

Art. 6º Para fins deste Decreto considera-se:

I - Apetite pelo Risco – quantidade e tipo de riscos que uma organização está preparada para buscar, manter ou assumir;

II - Atitude perante o Risco – abordagem da organização para analisá-lo e avaliá-lo e, com isso, decidir reduzir, evitar, compartilhar ou aceitar o risco;

III - Aversão ao Risco – atitude de afastar-se de riscos;

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

V - Controle – medida que visa a mitigação ou diminuir os efeitos do risco;

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

VII - 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;

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

IX - Fonte de Risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;

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

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

XII - Nível de Risco – magnitude de um risco expressa na combinação das consequências (impacto tido) e de suas probabilidades de ocorrência;

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

XIV - Perfil de Risco – descrição de um conjunto qualquer de riscos;

XV - Plano de Gestão de Riscos – esquema dentro de uma estrutura de gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;

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

XVII - Probabilidade – chance de algo acontecer;

XVIII - Processo de Avaliação de Riscos – processo global de identificação de riscos, análise de riscos e avaliação de riscos;

XIX - 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;

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

XXI - Riscos – efeito da incerteza nos objetivos organizacionais;

XXII - 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;

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

XXIV - Risco Residual – risco remanescente após o tratamento do risco;

XXV - 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:

I - Estratégicos – riscos decorrentes da falta de capacidade ou habilidade da Unidade em proteger-se ou adaptar-se às mudanças que possam interromper o alcance de objetivos e a execução da estratégia planejada;

II - De Conformidade – riscos decorrentes do órgão/entidade não ser capaz ou hábil para cumprir com as legislações aplicáveis ao seu negócio e não elabore, divulgue e faça cumprir suas normas e procedimentos internos;

III - Financeiros – riscos decorrentes da inadequada gestão de caixa, das aplicações de recursos em operações novas/desconhecidas e/ou complexas de alto risco;

IV - Operacionais – riscos decorrentes da inadequação ou falha dos processos internos, pessoas ou de eventos externos;

V - Ambientais – riscos decorrentes da gestão inadequada de questões ambientais, como por exemplo: emissão de poluentes, disposição de resíduos sólidos e outros;

VI - De Tecnologia da Informação – riscos decorrentes da indisponibilidade ou inoperância de equipamentos e sistemas informatizados que prejudiquem ou impossibilitem o funcionamento ou a continuidade normal das atividades da instituição. Representado, também, por erros ou falhas nos sistemas informatizados ao registrar, monitorar e contabilizar corretamente transações ou posições;

VII - De Recursos Humanos – riscos decorrentes da falta de capacidade ou habilidade da instituição em gerir seus recursos humanos de forma alinhada aos objetivos estratégicos definidos.

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

Parágrafo único. Os riscos identificados relacionados ao Combate à Corrupção deverão ser agrupados a fim de se avaliar o Nível de Risco consolidado, com vistas a priorizar as ações de tratamento adequados desses riscos;

Art. 8º São elementos estruturantes da gestão de riscos do município: a Política de gestão de riscos, o Comitê Municipal de *Compliance* Público, o Escritório de *Compliance*, o processo de gestão de riscos bem como seu controle e monitoramento.

CAPÍTULO V

Das Competências

SEÇÃO I

Disposições Gerais

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 do município.

SEÇÃO II

Das Responsabilidades pela Gestão de Riscos

Art. 10º Compete aos proprietários dos riscos:

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 quadrimestral) dos riscos ao Comitê de *Compliance* Público Municipal;

VII - verificar, periodicamente, se os controles existentes/implantados para mitigar os riscos são suficientes e adequados para manter o(s) risco(s) dentro do apetite a risco do município ou Secretaria.

Art. 11º Compete ao(s) coordenador(es) da Gestão de Risco e do Escritório de *Compliance* Público Municipal:

I - orientar e monitorar funções e responsabilidades pela gestão de riscos, especialmente com relação ao preenchimento da matriz de riscos e dos relatórios de gerenciamento de riscos pelos proprietários dos riscos;

II - monitorar as ações que estão em realização para evolução da maturidade em gestão de riscos;

III - orientar a integração do gerenciamento de riscos nos processos organizacionais e de gestão;

IV - centralizar informações referentes ao monitoramento da gestão de riscos;

V - comunicar ao Comitê de *Compliance* Público Municipal o andamento do gerenciamento de riscos; e

VI - acompanhar e monitorar os proprietários de riscos nas suas principais atribuições.

Art. 12º Compete ao Comitê de *Compliance* Público Municipal:

I - assegurar que a gestão de riscos está integrada aos processos de gestão, em especial, nas funções e atividades relevantes para o alcance dos objetivos-chaves do município;

II - fomentar as práticas de gestão de riscos;

III - definir o escopo da gestão de riscos;

IV - 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;

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

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

VII - definir e monitorar o apetite e a tolerância a riscos do município;

VIII - aprovar os riscos que deverão ser tolerados acima do apetite a risco do município;

IX - monitorar o cumprimento da política de gestão de riscos;

X - revisar a política de gestão de riscos;

XI - monitorar os indicadores-chaves de riscos nos processos de governança e gestão;

XII - estimular a cultura de gestão de riscos;

XIII - acompanhar o cumprimento de suas decisões;

XIV - definir e acompanhar o nível de maturidade em gestão de riscos almejado do município;

XV - acompanhar a implementação das ações dos eixos I, II e III do Programa de *Compliance* Público Municipal;

XVI - revisar periodicamente os riscos identificados no município, em contraste com o apetite a riscos, visando fornecer direção clara sobre o gerenciamento de riscos;

XVII - estabelecer parcerias com outras instituições/entes para tratar os riscos compartilhados.

CAPÍTULO VI

Do Processo de Gestão de Riscos

Art. 13º Serão adotados como referências técnicas para a gestão de riscos as normas ABNT NBR ISO 31000:2018, 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, visando definir o melhor tratamento para o risco;

VII - 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 - Monitoramento dos Riscos – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado;

X - Identificação dos Controles – identificação dos procedimentos, ações ou documentos que garantem o alcance dos objetivos do processo e diminuam a exposição aos riscos. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modifiquem o risco;

XI - Estabelecimento dos Controles – políticas e procedimentos que assegurem o alcance dos objetivos da administração, diminuindo a exposição das atividades aos riscos. Tais atividades acontecem ao longo do processo organizacional, em todos os níveis e em todas as funções, incluindo aprovações, autorizações, verificações, reconciliações, revisões de desempenho operacional, segurança de recursos e segregação de funções;

XII - 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;

XIII - 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.

Parágrafo único. Eventuais conflitos de atuação decorrentes do processo de gestão de riscos serão dirimidos pelo Comitê Municipal de *Compliance* Público.

Art. 14° O processo de gestão de riscos deve ser objeto de revisão periódica, sempre que necessário, com prazo não superior a um ano.

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, levando em consideração o limite máximo estipulado no *caput*.

CAPÍTULO VII

Disposições Finais

Art. 15º O Comitê de Compliance Público Municipal manterá registro formal de todos os atos administrativos provenientes do Programa de *Compliance* Público Municipal (PCM) a fim de fornecimento de dados para revisão periódica interna e para a consultoria.

Art. 16º Os proprietários dos riscos a que se refere o art. 9º deste Decreto deverão implantar a presente política de gestão de riscos a partir da data de publicação deste decreto.

Art. 17º Os casos omissos ou excepcionais serão resolvidos pelo Comitê de *Compliance* Público Municipal de acordo com as orientações a serem emanadas pela mentoria da CGE-GO ou TCMGO.

Art. 18º Este Decreto entra em vigor na data de sua publicação.

CUMPRA-SE e PUBLIQUE-SE.

GABINETE DO PREFEITO MUNICIPAL DE SANTA BÁRBARA DE GOIÁS, ESTADO DE GOIÁS, aos 27 dias do mês de maio de 2026.

JOB MARTINS DE DEUS
Prefeito Municipal

Job Martins de Deus
Prefeito Municipal
Santa Bárbara – GO