

PORTARIA Nº xx, DE xx DE XXXX DE 2022

Dispõe sobre a Política de Gestão de Riscos da **Secretaria de XXXXX do Distrito Federal – SIGLA**.

O SECRETÁRIO DE ESTADO DE **XXXXXX**, no uso das atribuições que lhe são conferidas pelo art. 105, parágrafo único, incisos I e III, da Lei Orgânica do Distrito Federal - LODF; considerando o Decreto nº 39.736, de 28 de março de 2019, o qual dispõe sobre a Política de Governança Pública e Compliance no âmbito da Administração Direta, Autárquica e Fundacional do Poder Executivo do Distrito Federal; considerando a Portaria nº **XX, de X de XXX de 20XX**, a qual institui o Comitê Interno de Governança da Secretaria de Estado **XXXXXX do Distrito Federal**, resolve:

Art. 1º Instituir a Política de Gestão de Riscos no âmbito da **Secretaria de XXXXXXX do Distrito Federal**, 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 parágrafo único do artigo 13 do Decreto nº 39.736, de 28 de março de 2019, que versa sobre a Política de Governança e Compliance no âmbito do Poder Executivo do Distrito Federal.

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 na **Secretaria de XXXXXXX do Distrito Federal**, 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 nesta Portaria deverá ser observada por todas as áreas e níveis de atuação da **Secretaria de XXXXX do Distrito Federal**, 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; e
- IV - o aprimoramento dos controles internos administrativos.

DOS PRINCÍPIOS DE GESTÃO DE RISCOS

Art. 5º A gestão de riscos observará os seguintes princípios:

- I – criar e proteger valores institucionais;
- II - ser parte integrante de todas as atividades organizacionais;
- III - ser estruturada e abrangente;
- IV - ser personalizada e proporcional aos contextos externo e interno da organização;
- V - ser inclusiva, envolvendo as partes interessadas;
- VI - ser baseada nas melhores informações disponíveis;
- VII - considerar fatores humanos e culturais;
- VIII - ser dinâmica, interativa e capaz de reagir a mudanças; e
- IX - facilitar a melhoria contínua da organização.

DAS DIRETRIZES DE GESTÃO DE RISCOS

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

- I - Riscos - efeito da incerteza nos objetivos a serem atingidos pela instituição;
- II - Gestão de Riscos - atividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco;
- III - Estrutura de Gestão de Risco - conjunto de elementos que fornecem os fundamentos e disposições organizacionais para conceber, implementar, monitorar, rever e melhorar continuamente a gestão do risco em toda a organização;
- IV - Política de Gestão de Risco - declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;
- V - Atitude perante o Risco - abordagem da organização para avaliar e eventualmente buscar, manter, assumir ou afastar-se do risco;
- VI - Apetite pelo Risco - quantidade e tipo de riscos que uma organização está preparada para buscar, manter ou assumir;
- VII - Aversão ao Risco - atitude de afastar-se de riscos;
- VIII - 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;
- IX – Proprietário/Gerente de Risco - pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;
- X - 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;
- XI - Parte Interessada - pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;
- XII - Processo de Avaliação de Riscos - processo global de identificação de riscos, análise de riscos e avaliação de riscos;

- XIII - Fonte de Risco - elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;
- XIV - Evento - ocorrência ou alteração em um conjunto específico de circunstâncias;
- XV - Consequência - resultado de um evento que afeta os objetivos;
- XVI - Probabilidade - chance de algo acontecer;
- XVII - Nível de Risco - magnitude de um risco expressa na combinação das consequências e de suas probabilidades;
- XVIII - Controle - medida que está modificando o risco;
- XIX - Risco Residual - risco remanescente após o tratamento do risco;
- XX - Risco Inerente - risco ao qual se expõe face à inexistência de controles que alterem o impacto ou a probabilidade do evento;
- XXI - Tolerância ao Risco - é o nível de variação aceitável quanto à realização dos seus objetivos; e
- XXII - Impacto - efeito resultante da ocorrência do evento.

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 elaborar, divulgar e fazer 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, das pessoas ou de eventos externos;
- V - Ambientais: riscos decorrentes da gestão inadequada de questões ambientais, como: emissão de poluentes, disposição de resíduos sólidos e outros;
- VI - De Tecnologia da Informação: riscos decorrentes da inexistência, 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 - De Integridade: riscos decorrentes da não aderência aos valores, princípios e normas éticas da instituição, principalmente àqueles ligados a fraudes e a atos de corrupção.

Art. 8º São elementos estruturantes da Gestão de Riscos da **Secretaria de XXXX do Distrito Federal** a Política de Gestão de Riscos, o Comitê Interno de Governança, o Processo de Gestão de Riscos e o 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 desenvolvidos na **Secretaria de XXXXXX do Distrito Federal**.

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

I – indicar para aprovação da **Instância de Governança do Órgão** os processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, considerando a dimensão dos prejuízos que possam causar;

II – propor à **Instância de Governança do Órgão** quais riscos deverão ser priorizados para tratamento por meio de ações de caráter imediato, a curto, médio ou longo prazos ou de aperfeiçoamento contínuo;

III – propor e acompanhar a implementação das ações de tratamento a serem implementadas, assim como o prazo de implementação e avaliação dos resultados obtidos; e

IV - fornecer as informações sobre o gerenciamento dos riscos sob sua responsabilidade.

DO PROCESSO DE GESTÃO DE RISCOS

Art. 11. Serão adotadas como referências técnicas para a gestão de riscos as normas ABNT NBR ISO 31000:2018, ABNT ISO 19001:2011 agregadas ao COSO 2017 - Controles Internos - Estrutura Integrada, compreendido pelas seguintes fases:

I - Comunicação e Consulta - processos contínuos e iterativos 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 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;

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

IV - 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;

V - 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;

VI - Tratamento dos Riscos - processo para modificar o risco;

VII - 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;

VIII - Identificação dos Controles - identificação dos procedimentos, ações ou documentos que garantem o alcance dos objetivos do processo e diminuem a exposição aos riscos; e

IX - 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 recurso e segregação de funções.

Parágrafo único. Eventuais conflitos de atuação decorrentes do processo de gestão de riscos serão dirimidos pelo Comitê Interno de Governança.

Art. 12. O processo de gestão de riscos deve ser realizado em ciclos não superiores a 1 (um) ano abrangendo os processos de trabalho das áreas de gestão da **Secretaria de XXXXXX do Distrito Federal**.

DAS DISPOSIÇÕES GERAIS

Art. 13. O gerenciamento dos riscos na **Secretaria de XXXXXX do Distrito Federal** será feito por meio do Sistema de Gestão de Auditoria do Distrito Federal (Saeweb) ou de outro que vier a substituí-lo.

Art. 14. Os artefatos produzidos na gestão de riscos, quais sejam, o contexto, a matriz de riscos e o plano de ação, são considerados documentos preparatórios para tomada de decisão pela gestão da **Secretaria de XXXXXX do Distrito Federal**.

Parágrafo único. Por se tratar de documentos preparatórios, podem conter informações sensíveis que, caso divulgadas indevidamente, podem prejudicar ou causar riscos para o desenvolvimento das atividades de interesse estratégico da **Secretaria de XXXXXX do Distrito Federal**, devendo ser resguardado seu sigilo dentro dos parâmetros normativo.

Art. 15. Os casos omissos ou excepcionais serão resolvidos pelo Comitê Interno de Governança de acordo com as orientações a serem emanadas da Controladoria-Geral do Distrito Federal - CGDF.

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