MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS
PROCURADORIA-GERAL DE JUSTIÇA

PORTARIA NORMATIVA N.º 587 , DE 7 DE NOVEMBRO DE 2018

Institui a Política de Gestão de Risco de Tecnologia da Informação no âmbito do Ministério Público do Distrito Federal e Territórios.

O **PROCURADOR-GERAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS,** no uso das atribuições legais conferidas pela Lei Complementar n.° 75, de 20 de maio de 1993,

CONSIDERANDO a Política de Governança e Gestão de Tecnologia da Informação – PGTI instituída pela Portaria Normativa n ° 552, de 20 de junho de 2018;

CONSIDERANDO a Portaria PGR/MPU nº 78, de 8 de agosto de 2017, que instituiu a Política de Gestão de Riscos do Ministério Público da União;

CONSIDERANDO a necessidade de estabelecer diretrizes para elaboração e manutenção de um processo de gestão de risco de TI alinhado com a gestão de risco da Instituição e equilibrar custos e benefícios da gestão de risco de TI,

RESOLVE:

Art. 1º Instituir a Política de Gestão de Risco de Tecnologia da Informação – PGRTI no âmbito do MPDFT.

Art. 2º A PGRTI/MPDFT observará conceitos, objetivos, princípios, diretrizes, papéis e responsabilidades estabelecidos nesta portaria, bem como as disposições constitucionais, legais e regimentais vigentes.

CAPÍTULO I
DOS CONCEITOS

Art. 3º Para os efeitos do presente ato, considera-se:

I – apetite ao risco: nível de risco que a Instituição considera aceitável;

II – catálogo de serviços de TI: banco de dados ou documento estruturado contendo informações sobre os serviços de TI ativos;

III – evento: ocorrência, interna ou externa, capaz de causar impacto em objetivos estratégicos, programas, projetos, processos de trabalho ou iniciativas institucionais;

IV – natureza do risco: tipo do risco (financeiro, patrimonial, ético, de imagem, de conformidade etc);

V – nível de risco: magnitude do risco, obtida a partir do produto da probabilidade de ocorrência do risco pelo seu impacto;

VI – processos críticos de trabalho: são aqueles sem os quais as funções essenciais do MPDFT ao cidadão não podem ser exercidas;

VII – risco de TI: efeito da incerteza em projetos, iniciativas ou serviços de TI caracterizado por uma possível alteração negativa em relação ao resultado esperado;

VIII – serviço de TI: uma ou mais soluções de TI que, em conjunto, habilitam um processo de negócio.

CAPÍTULO II
DOS OBJETIVOS

Art. 4º A PGRTI tem por objetivo geral:

I – assegurar o alinhamento do processo de gestão de risco de TI com a gestão de risco da Instituição;

II – identificar, avaliar e reduzir continuamente o risco relacionado à TI dentro dos níveis de tolerância estabelecidos pela alta administração da instituição;

III – promover o balanceamento adequado entre os custos e os benefícios da Gestão dos Riscos de TI.

CAPÍTULO III
DAS DIRETRIZES

Art. 5º A Gestão de Risco de TI deve ser:

I – aplicada a projetos, iniciativas e serviços críticos de TI;

II – incorporada ao processo de tomada de decisões dentro da Secretaria de Tecnologia da Informação – STI e ao Comitê Estratégico de Tecnologia da Informação – CETI.

§1º Os projetos e as iniciativas são os constantes no Plano Diretor de Tecnologia da Informação – PDTI.

§2º Os serviços críticos de TI são aqueles que dão suporte aos processos críticos de trabalho e constam no catálogo de serviço de TI.

CAPÍTULO IV
DOS PAPÉIS E DAS RESPONSABILIDADES

Art. 6º A implementação da gestão de risco ficará a cargo do subsecretário de TI responsável pelo objeto de avaliação do risco, ocasião em que exercerá o papel de Gestor de risco.

Art. 7º Compete ao gestor de risco, relativamente aos objetos de avaliação de riscos sob sua responsabilidade:

I – escolher, justificadamente, dentre os objetos sob sua responsabilidade previstos no art. 5º quais terão os riscos gerenciados, considerando a dimensão dos prejuízos que possam causar;

II – assegurar que os riscos sejam gerenciados de acordo com os critérios estabelecidos nesta Portaria;

III – monitorar informações adequadas sobre a gestão de riscos e reportá-las às partes interessadas.

CAPÍTULO V
DA GESTÃO DE RISCO DE TI

Art. 8º A Gestão de Risco de TI é um processo que deve ser executado considerando, no mínimo, as seguintes etapas:

I – identificar e descrever os riscos de TI: consiste na busca, no reconhecimento e na descrição de riscos, mediante a identificação de fontes, eventos, causas e potenciais consequências. Essa ação é validada mediante:

a. registro dos riscos identificados em documento, planilha ou sistema, sempre de forma padronizada e gerenciável.

II – avaliar os riscos de TI: compreender a natureza do risco e determinar o respectivo nível de risco mediante a combinação da probabilidade de sua ocorrência e dos possíveis impactos, observando os seguintes critérios:

a) o risco de TI deve ser classificado quanto a sua natureza: financeiro, patrimonial, ético, de imagem ou de conformidade;

b) a probabilidade de o risco de TI ocorrer deverá ser classificada como baixa, média e alta;

c) o impacto deverá ser classificado como pequeno, intermediário ou grande;

d) os níveis de riscos devem ser classificados, após análise da combinação entre probabilidade e impacto, como sendo de baixa gravidade, média gravidade ou alta gravidade.

III – tratar os riscos de TI: consiste na seleção e na implementação de uma ou mais ações de tratamento para abordar os riscos. No desempenho dessa ação, consideram-se as seguintes condições:

a) as ações de tratamento de riscos terão os objetivos de evitar, mitigar, transferir ou aceitar o risco;

b) as propostas de tratamento dos riscos de TI devem ser aprovadas pelo CETI, quando tratarem de projetos, iniciativas ou serviços que deem suporte aos processos críticos de trabalho, ou pelo secretário de TI nos demais casos.

IV – monitorar e comunicar: verificar continuamente se os riscos se concretizaram, se as ações de tratamento propostas foram executadas e se houve sucesso no tratamento ou na mitigação dos riscos de TI e comunicar os resultados às partes interessadas com base nos critérios a seguir:

a) a comunicação deve ser periódica e por meio da apresentação de relatório;

b) a frequência da comunicação deve ser definida junto com as partes interessadas.

V – melhorar continuamente: a partir da análise dos resultados do monitoramento, propor, quando for o caso, melhorias para a gestão de isco,, considerando que:

a) riscos antes aceitáveis, por exemplo, podem ser reclassificados e tratados com outras ações;

b) novos riscos podem ser identificados e gerenciados.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 9º Deverão ser desenvolvidas e implantadas estratégias de:

I – sensibilização da Instituição quanto à importância da Gestão de Risco de TI para o alcance dos objetivos estratégicos;

II – comunicação entre as partes envolvidas, visando ampliar a participação e a transparência nas ações do processo de Gestão de Risco de TI dentro da STI.

Art. 10. Esta Portaria Normativa entrará em vigor na data de sua publicação.

Dê-se ciência, cumpra-se e publique-se.

LEONARDO ROSCOE BESSA