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

PORTARIA NORMATIVA Nº 584 , DE 29 DE OUTUBRO DE 2018

Institui a Política de Gestão de Continuidade dos Serviços de TI 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 nº 75, de 20 de maio de 1993,

CONSIDERANDO a Política de Governança e Gestão de Tecnologia da Informação – PGTI, instituída pela Portaria Normativa N º 522, de 20 de julho de 2018;

CONSIDERANDO a necessidade de estabelecer diretrizes para elaboração e manutenção de um Plano de Continuidade de TI que permita que a Secretaria de Tecnologia da Informação – STI responda o mais rapidamente possível a interrupções graves, de forma a continuar a execução dos serviços de TI que apoiam os processos críticos de trabalho do Ministério Público do Distrito Federal e Territórios – MPDFT;

CONSIDERANDO o teor do Procedimento de Gestão Administrativa nº 08191.109450/2018-14,

RESOLVE:

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

Art. 2º A PGCTI/MPDFT observará os conceitos, objetivos, princípios, diretrizes, papéis e responsabilidades estabelecidos neste Ato, bem como as disposições constitucionais, legais e regimentais vigentes.

CAPÍTULO I
DOS CONCEITOS

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

I – Acordo de Nível de Serviço (ANS): contrato, termo ou acordo entre o provedor de serviços de TI e seus clientes. Descreve condições e garantias na prestação dos serviços de TI, documenta metas de qualidade e especifica as responsabilidades do provedor de serviços de TI e seus clientes;

II – Ativo de TI: qualquer componente ou recurso que precise ser gerenciado de forma a garantir a entrega de um serviço de TI;

III – Catálogo de Serviços de TI: banco de dados ou documento estruturado contendo informações sobre os serviços de TI ativos;

IV – Incidente: interrupção ou redução da qualidade, não planejadas, de serviços de TI;

V – Desastre: acontecimento de grandes proporções que causa interrupção e inviabiliza o funcionamento adequado dos serviços de TI por tempo indeterminado;

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

CAPÍTULO II
DOS OBJETIVOS E DIRETRIZES

Art. 4º A PGCTI tem por objetivo estabelecer diretrizes para a elaboração e a manutenção do Plano de Continuidade de TI.

§ 1º O Plano de Continuidade de TI tem por objetivo restaurar, dentro do menor tempo possível, os serviços de TI essenciais para que a instituição continue funcionando e, assim, diminuir os impactos de um desastre.

§ 2º O Plano de Continuidade de TI deve:

I – Estar alinhado com a Gestão de Risco e o Plano de Continuidade do Negócio – PCN da instituição;

II – Prover mecanismos para contribuir com o cumprimento da missão do MPDFT diante de um acontecimento desastroso;

III – Ter definidos os papéis e responsabilidades para execução dos procedimentos de continuidade.

CAPÍTULO III
DO PLANO DE CONTINUIDADE DE TI

Art. 5º O Plano de Continuidade de TI é um conjunto de mecanismos e procedimentos que orientam a unidade de TI a responder, recuperar, retornar e restaurar os serviços de TI que apoiam os processos críticos de trabalho para um nível predefinido de operação, após um desastre.

Art. 6º O Plano de Continuidade de TI deve ser elaborado em seis etapas:

I – Identificação dos processos críticos de trabalho;

II – Identificação dos serviços de TI que dão suporte aos processos críticos de trabalho;

III – Avaliação de risco;

IV – Definição e implementação da solução de contingência;

V – Elaboração do Plano de Recuperação de Desastre;

VI – Testes, treinamento e manutenção.

SEÇÃO I
IDENTIFICAÇÃO DOS PROCESSOS CRÍTICOS DE TRABALHO

Art. 7º Os processos críticos de trabalho devem ser identificados com a alta administração e em consonância com o PCN e com o Planejamento Estratégico da Instituição – PEI.

§1º Na ausência de um PCN, a alta administração pode designar órgão colegiado, comitê ou comissão para apoiar na identificação desses processos.

§ 2º Os processos críticos de trabalho são aqueles sem os quais as funções essenciais do MPDFT perante o cidadão não podem ser exercidas.

SEÇÃO II
IDENTIFICAÇÃO DOS SERVIÇOS DE TI

Art. 8º Elaborar um mapa relacionando os serviços de TI que dão suporte aos processos críticos de trabalho identificados na etapa anterior.

Parágrafo Único. Este mapa deve incluir, no mínimo:

I- Nome do serviço de TI, conforme apresentado no Catálogo de Serviços de TI, previsto na Portaria Normativa nº 127, de 27 de setembro de 2010;

II- Ativos de TI que compõem cada serviço de TI e seus relacionamentos, conforme previsto na Portaria Normativa nº 124, de 20 de dezembro de 2016;

III- Nome dos processos críticos de trabalho a que dão suporte;

IV- Nome da pessoa ou da unidade organizacional responsável pelo processo crítico de trabalho;

V- Nome da pessoa ou da unidade organizacional responsável pelo serviço de TI.

SEÇÃO III
AVALIAÇÃO DE RISCO

Art. 9º A avaliação de risco deve ser feita com o intuito de identificar os eventos que podem causar indisponibilidades graves nos serviços de TI que apoiam os processos críticos de trabalho, seus impactos e a probabilidade de eles ocorrerem.

§ 1º A avaliação de risco deve ser realizada de acordo com o previsto na Portaria PGR/MPU nº 78, de 8 de agosto de 2017;

§ 2º As soluções de contingência devem ser providenciadas para os serviços de TI em que haja ocorrência de eventos classificados com média ou alta probabilidade de ocorrer e cuja indisponibilidade gere grandes impactos nos processos críticos de trabalho.

SEÇÃO IV
SOLUÇÃO DE CONTINGÊNCIA

Art. 10 A solução de contingência consiste em definir quais os mecanismos que serão adotados para prover um ambiente backup para os serviços de TI que necessitam ser incluídos no Plano de Continuidade de TI.

Art. 11 O ambiente backup é de um local alternativo, distinto e distante do local onde o serviço de TI funciona primariamente, no qual serão instalados e mantidos os serviços de TI e seus ativos de forma secundária, a um custo justificável, de acordo com a avaliação de risco feita anteriormente.

Art. 12 Fica a cargo da STI definir o local do ambiente backup, sua infraestrutura, como será mantido e quais os critérios que devem ser atendidos em termos de segurança, capacidade e disponibilidade, em conformidade com as normas internas vigentes.

Parágrafo único. Fica a cargo do CETI aprovar a solução de contingência apresentada pela STI.

Art. 13 Em situações de contingência, os Acordos de Níveis de Serviço estabelecidos, conforme Portaria Normativa nº 127, de 27 de setembro de 2010, poderão não ser atendidos em sua totalidade, uma vez que os serviços podem não estar sendo oferecidos com sua capacidade originalmente planejada para funcionamento em situações normais.

Art. 14 A solução de contingência deve ser acionada quando da ocorrência do desastre e deve ficar operacional até que este seja resolvido e o ambiente primário tenha sido restabelecido.

SEÇÃO V
ELABORAÇÃO DO PLANO DE RECUPERAÇÃO

Art. 15 Fica a cargo da STI elaborar o Plano de Recuperação, e o CETI é responsável por aprová-lo.

Parágrafo único: O Plano de Recuperação é um documento, na forma de processo ou de matriz RACI, que detalha as instruções necessárias para o acionamento da solução de contingência e deve conter, no mínimo:

I- Papéis e responsabilidades, indicando quem são os responsáveis por acionar a solução de contingência e suas respectivas ações;

II- As ações que serão executadas de forma automática e as que precisam ser executadas de forma manual.

SEÇÃO VI
TESTES, TREINAMENTO E MANUTENÇÃO

Art. 16 Para garantir que a Solução de Contingência funcione em situação de desastre, ela e o Plano de Recuperação precisam ser testados periodicamente.

Parágrafo único. Fica a cargo da STI:

I- Criar e executar periodicamente as rotinas de testes da Solução de Contingência e reportar os resultados ao CETI;

II- Treinar as pessoas envolvidas no Plano de Recuperação, de forma que todos conheçam seus papéis e responsabilidade quando a Solução de Contingência tiver de ser acionada.

Art. 17 O Plano de Continuidade deve ser continuamente revisado para refletir, quando houver, as alterações nos processos críticos de trabalho e/ou nos serviços de TI que o apoiam.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 18 Deverão ser desenvolvidas e implantadas estratégias de sensibilização da instituição quanto à importância do Plano de Continuidade de TI;

Art. 19 A implementação do disposto nesta Portaria fica a cargo da Secretaria de Tecnologia da Informação.

Art. 20 Esta Portaria Normativa entrará em vigor na data de sua publicação.

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

LEONARDO ROSCOE BESSA