MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Resolução CETI n.º 6, de 7 de março de 2016.

Estabelece metas e estrutura para a gestão da Continuidade de Serviços de Tecnologia da Informação no Ministério Público do Trabalho conforme diretrizes da Política Nacional de Segurança da Informação.

O COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI) do Ministério Público do Trabalho, no uso das atribuições que lhe conferem a Portaria n.º 723, de 9 de setembro de 2015;

CONSIDERANDO que, de acordo com a Resolução CNMP n.º 70, compete ao CETI definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de Tecnologia da Informação;

CONSIDERANDO a necessidade de aprimorar os padrões de governança em Tecnologia da Informação no Ministério Público do Trabalho;

CONSIDERANDO os padrões ABNT/NBR ISO 22.301 (Segurança da Sociedade - Sistema de Gestão de Continuidade de Negócios – Requisitos), ABNT/NBR ISO 22.313 (Segurança da Sociedade - Sistema de Gestão de Continuidade de Negócios – Orientações), ISO/IEC 27.000 (*Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabular*), ABNT/NBR ISO/IEC 27.001 (Tecnologia da Informação - Técnicas de segurança - Sistema de Gestão da Segurança da Informação – Requisitos), ABNT/NBR ISO/IEC 27.002 (Tecnologia da Informação - Técnicas de segurança - Código de Prática para Controles de Segurança da Informação) e ABNT/NBR ISO/IEC 27.031 (Tecnologia da Informação - Diretrizes para a Prontidão para a Continuidade dos Negócios da Tecnologia da Informação e Comunicação);

CONSIDERANDO as diretrizes da Resolução CETI n.º 4/2016, que institui a Política Nacional de Segurança da Informação do Ministério Público do Trabalho;

CONSIDERANDO a necessidade de garantir a disponibilidade e a integridade dos sistemas e das informações corporativas, em especial no que tange ao portfólio do MPT Digital (integrado ao Processo Judicial Eletrônico da Justiça do Trabalho mediante mecanismos de interoperabilidade) e do MPT Cosmos;

CONSIDERANDO a necessidade de estabelecer diretrizes para a criação dos Planos de Continuidade de Serviços de Tecnologia da Informação;

RESOLVE

Art. 1º Estabelecer diretrizes e padrões para planejar, desenvolver, testar, ativar, monitorar e manter a Gestão da Continuidade de Serviços de Tecnologia da Informação (TI), doravante GCSTI, no âmbito do Ministério Público do Trabalho (MPT), nos termos desta Resolução.

§1º Entende-se por GCSTI o conjunto de processos definidos para:

I. Identificar o nível mínimo aceitável da continuidade de operações dos serviços de TI;

II. Estimar riscos e analisar impactos negativos derivados da eventual ocorrência de incidentes de segurança da informação;

III. Descrever estratégias de implementação dos Planos de Continuidade de Serviços de TI – PCSTI.

§2º A operação dos serviços de TI compreende todas as atividades correlatas de coordenação e de execução, de acordo com os níveis de qualidade definidos e com o suporte da infraestrutura tecnológica do MPT.

CAPÍTULO I

DO PLANEJAMENTO

Art. 2º O planejamento dos processos de continuidade de serviços, com a participação necessária de seus gestores, compreende as seguintes atividades:

I. Definição do escopo de atuação da continuidade de negócio, com foco em toda a cadeia de dependência da plataforma operacional;

II. Identificação dos requisitos de segurança da informação;

III. Determinação do nível de criticidade e dos níveis aceitáveis de disponibilidade;

IV. Definição do tempo máximo aceitável de perda de informação.

V. Incorporação sistêmica de análises de risco e de impacto.

Parágrafo Único. No âmbito de suas áreas de atuação, os gestores, custodiantes e administradores deverão manter a base de dados de gestão da configuração atualizada com informações derivadas da transição de novos serviços, da mudança de serviços pré-existentes ou da retirada de operação de serviços em funcionamento.

Art. 3º As análises de risco e de impacto serão destinadas à identificação de medidas preventivas de incidentes, de ações corretivas e de providencias de mitigação de efeitos negativos, sobretudo para reduzir ao máximo os períodos de eventual interrupção.

Art. 4º A análise de riscos operacionais deverá fornecer ao planejamento da continuidade de serviços de TI os seguintes elementos de informação:

I. Avaliação dos riscos que podem afetar a disponibilidade dos serviços de TI;

II. Resultado dos processos de análise de riscos, conforme norma específica;

III. Cadeia de dependências da plataforma operacional;

IV. Identificação das ações, para tratamento de incidentes, que devam ser consideradas nos PCSTI.

Parágrafo Único. A análise a que se refere o caput deverá ser organizada em processo estruturado de identificação, avaliação e tratamento de riscos operacionais incidentes sobre os serviços de TI com a finalidade de fornecer ao gestor uma compreensão objetiva do esforço necessário para reduzi-los a níveis aceitáveis.

Art. 5º A análise de impacto deverá fornecer ao planejamento da continuidade de serviços de TI os seguintes elementos de informação:

I. Avaliação das consequências do não cumprimento dos níveis de disponibilidade previamente definidos para os serviços;

II. Definição da cadeia de prioridade para a retomada dos níveis de disponibilidade nos casos de ocorrência de incidentes que afetem mais de um serviço ou componente da plataforma tecnológica.

Art. 6º O planejamento dos processos de continuidade de serviços de TI deverá prever e indicar:

I. Estimativa de custos financeiros necessários à garantia dos processos de continuidade;

II. Recursos humanos e técnicos necessários;

III. Restrições da plataforma tecnológica que possam causar impactos negativos.

Art. 7º As competências técnicas de servidores e colaboradores do MPT relativas ao escopo de atuação em prol da continuidade dos serviços de TI deverão ser adequadamente mapeadas para garantir a exequibilidade das ações previstas nos planos.

§ 1º Nos contratos de prestação de serviço, devem ser mapeados e atualizados os contatos técnicos, os regimes de prestação de serviço e o Acordo de Nível de Serviço das respectivas equipes de suporte.

§ 2º A manutenção de informações unificadas sobre contratos de prestação de serviços e do mapa de competências será de responsabilidade conjunta dos dirigentes da TI-PGT e da TI-Regional, respeitados os padrões da Resolução CETI n. 2/2016.

CAPÍTULO II

DAS ESTRATÉGIAS PARA A CONTINUIDADE DE SERVIÇOS DE TI

Art. 8º A definição das estratégias de continuidade de serviços de TI será baseada nas informações produzidas na fase de planejamento, a fim de garantir o alinhamento com as reais necessidades do MPT.

Art. 9º Cada PCSTI será desenvolvido e aprimorado continuamente, com revisão anual, para:

I. Determinar critérios e procedimentos de sua ativação ou renovação;

II. Estabelecer protocolos apropriados de comunicação interna e externa;

III. Especificar rol de medidas imediatas que devam ser adotadas na ocorrência de eventos de indisponibilidade;

IV. Estabelecer procedimentos flexíveis para responder a ocorrências imprevistas, inclusive potenciais, com aptidão de adaptação a mudanças nas condições internas e externas;

V. Manter o foco na prevenção do impacto negativo das ocorrências sobre as atividades do MPT, conforme a criticidade dos sistemas, dos serviços e das infraestruturas;

VI. Definir rotinas para teste de monitoramento dos indicadores-chave de risco e de efetividade da resposta a eventos;

VII. Definir rotinas de monitoramento dos itens de configuração da plataforma tecnológica.

Art. 10 Em consonância com a estratégia para a continuidade de serviços TI, serão elaborados:

I. PCSTI específico para cada serviço crítico, a incluir aspectos de infraestrutura, processamento e rede;

II. PCSTI para tratar especificamente do conjunto de serviços não críticos.

Parágrafo Único: A responsabilidade pela implementação, operação, monitoramento e manutenção dos PCSTI será da TI-PGT, que poderá delegar atribuições, conforme o caso, a equipe gestora do serviço de TI, composta por integrantes da TI-PGT e da TI-Regional.

Art. 11 Sempre que necessária a implementação do PCSTI em instalações ou localidades alternativas, os seguintes requisitos deverão ser observados:

I. Verificação da existência de instalações ou localidades alternativas sob responsabilidade da unidade do MPT;

II. Verificação da possibilidade de outra unidade do MPT fornecer instalações;

III. Verificação da existência, na mesma localidade da unidade do MPT, de unidades de outros ramos do MPU que possam ceder ou compartilhar instalações.

IV. Verificação da necessidade de implementação do PCSTI em outra localidade ou em instalações de terceiros.

§1º As diretrizes de segurança física da Política Nacional de Segurança da Informação deverão ser respeitadas.

§2º Deverá ser providenciado, com antecedência razoável, o acesso físico e lógico da equipe técnica da unidade do MPT que implementará o PCSTI.

§3º Paralelamente às estratégias de localidade e de instalações, dever-se-á verificar a viabilidade de manter infraestrutura de processamento, dados e redes nos seguintes regimes:

I. Infraestrutura replicada e atualizada para pronta entrega de serviços (hot site);

II. Infraestrutura parcialmente preparada, a requerer tempo para ativação, replicação e atualização dos serviços (warm site);

III. Infraestrutura não preparada, a demandar tempo para sua total implementação total (cold site).

Art. 12 Consideram-se as seguintes definições de parâmetros, a serem utilizadas nos PCSTI, em consonância com a literatura técnica:

I. Ponto Pretendido para Recuperação (RPO - Recovery Point Objective): tempo ou volume de informação a ser garantido após um incidente de segurança;

II. Tempo Pretendido para Recuperação (RTO - Recovery Time Objective): tempo entre o início da indisponibilidade e o retorno do serviço à operação;

III. Tempo para Recuperação Plena (WRT - Work Recovery Time): tempo, após o RTO, necessário para a restauração de cópias de segurança ou para a replicação de bases de dados, considerada a meta de operação em consonância com os níveis de qualidade de serviço acordados;

IV. Tempo Máximo Tolerável (MTD - Maximum Tolarable Dowtime): tempo máximo de indisponibilidade, considerada a soma do tempo RTO e do tempo WRT.

Parágrafo Único. O parâmetro RPO deverá ser considerado na configuração dos intervalos das cópias de segurança dos dados dos serviços.

Art. 13 A implementação prévia de medidas e regras de segurança, considerado o perfil de risco, constitui requisito a ser verificado na descrição dos procedimentos específicos da continuidade de serviços de TI.

CAPÍTULO III

DO DESENVOLVIMENTO DO PCSTI

Art. 14 Os planos (PCSTI) serão compilados em documento formal que sistematizará os procedimentos para a continuidade dos serviços de TI de acordo com a seguinte estrutura:

I. Abordagem do propósito e do escopo do PCSTI em relação à:

a) criticidade do serviço;

b) conformidade legal ou normativa;

c) descrição geral da plataforma tecnológica com a respectiva documentação;

II. Descrição do objetivo do PCSTI, com definição dos parâmetros de RPO, RTO, WRT e MTD;

III. Definição dos papeis e das responsabilidades;

IV. Indicação dos recursos tecnológicos necessários;

V. Exposição dos critérios para ativação do plano;

VI. Exposição do plano de Recuperação do Serviço de TI (PRSTI);

VII. Definição de critérios para aceitação do RTO e WRT;

VIII. Delineamento do plano de comunicação, com previsão de que todas as demandas externas ou de imprensa deverão ter seu atendimento intermediado pelas Assessorias de Comunicação Social.

§1º O propósito, o escopo e o objetivo deverão ter por base as informações coletadas na fase de planejamento.

§2º O dirigente da unidade do MPT, exceto se designado outro profissional pela TI-PGT, mediante solicitação fundamentada da TI-Regional, será o responsável local pelo PCSTI, considerados os seguintes aspectos:

I. Gerência de níveis de serviços;

II. Gerência de níveis de operações;

III. Gestão de riscos;

IV. Gestão de operações, capacidade e disponibilidade;

V. Acompanhamento de indicadores de desempenho (KPI) e de risco (KRI) locais não atribuídos a outras áreas ou equipes.

Parágrafo Único. Incumbe ao dirigente da TI-PGT promover compilações analíticas e comparativas da situação dos itens I a V em âmbito nacional.

Art. 15 A documentação da arquitetura tecnológica deve considerar a localidade, o regime das instalações e os critérios de aceitação do RTO e do WRT.

§1º Durante o desenvolvimento do plano, o gestor do serviço de TI será informado na hipótese de detecção de falta ou de limitação de recursos que necessários à ativação do PCSTI.

§2º Se a falta ou a limitação incidir sobre serviços críticos, o CETI será cientificado com proposta de providências.

Art. 16 No PCSTI, devem ser considerados os seguintes eventos, quanto ao comprometimento do serviço:

I. Os evidenciados pelo registro de incidentes ou por indicadores de desempenho:

a) de indisponibilidade total;

b) de indisponibilidade parcial que prejudique os níveis acordados de qualidade do serviço;

c) de comprometimento da confidencialidade ou da integridade das informações.

II. Os danos potenciais, monitorados por indicadores de risco (KRI), que apontem tendências de comprometimento de disponibilidade, de confidencialidade ou de integridade das informações.

Art. 17 A informação necessária para localização de agentes e responsáveis que atuem no interesse do PCSTI e de planos de resposta deverá ser mantida atualizada no serviço de diretório.

Parágrafo Único. O repositório de informações de agentes e responsáveis deverá conter, no mínimo, o horário de trabalho, atualizado de forma colaborativa, e os registros relativos ao atendimento dos serviços de suporte terceirizados.

Art. 18 O Plano de Recuperação do Serviço de TI (PRSTI) deverá descrever objetivamente os procedimentos técnicos necessários para a recuperação do serviço, de forma a considerar, respeitados os padrões da Resolução CETI n.º 2/2016:

I. A dimensão do problema e seus impactos imediatos;

II. O potencial de agravamento do problema;

III. A verificação dos parâmetros acordados de RPO, RTO, WRT e MTD e a estimativa destes diante do problema;

IV. A referência aos registros, em base de conhecimento, que versem sobre:

a) alternativas para solução imediata de contorno;

b) atividades para solução do problema da causa raiz;

c) atividades de recuperação;

d) atividades para restauração das cópias de segurança.

§1º Todos os registros da base de conhecimento devem contemplar as ações para verificação da eficácia da solução, bem como o responsável pela validação da resolução do incidente.

§2º A desmobilização dos agentes envolvidos na resposta ao evento deverá ocorrer na forma da Resolução CETI n.º 2/2016.

CAPÍTULO IV

DOS TESTES DO PCSTI

Art. 19 O PCSTI deve ser testado com base nos seguintes objetivos:

I. Construir confiança, em todo o MPT, de que as estratégias de continuidade de serviços de TI atendem às necessidades da instituição;

II. Demonstrar que os serviços críticos podem ser mantidos e recuperados dentro dos níveis estabelecidos no planejamento da continuidade;

III. Proporcionar às equipes técnicas a oportunidade de exercitarem suas habilidades e competências em situações de simulação de crise;

IV. Verificar se o PCSTI está em conformidade com os requisitos operacionais do serviço de TI;

V. Identificar novas vulnerabilidades, ameaças e impactos negativos que poderão subsidiar uma nova interação da análise de risco operacional.

Art. 20 A programação dos testes do PCSTI deverá compreender as seguintes etapas:

I. Definição de escopo, cenários possíveis e objetivos a serem alcançados;

II. Levantamento dos recursos humanos e tecnológicos necessários para execução do teste;

III. Planejamento das atividades do teste;

IV. Implementação do teste;

V. Relatório analítico do teste.

Art. 21 Os testes deverão contemplar escopos que avultem de diferentes cenários em variados graus de complexidade e criticidade, com base nas informações das análises de risco e de impacto aos serviços.

§ 1º O escopo de baixa complexidade deverá obrigatoriamente contemplar testes de restauração das cópias de segurança.

§ 2º Os ritos de teste devem ser comunicados previamente ao gestor do serviço de TI, de modo que este promova a multiplicação das informações relevantes à compreensão, pelos interessados, de eventuais impactos.

CAPÍTULO V

DO MONITORAMENTO E DA MANUTENÇÃO DO PCSTI

Art. 22 O monitoramento do PCSTI em execução deverá registrar, no mínimo, as seguintes informações:

I. A descrição de problemas;

II. Os procedimentos do PCSTI necessários para o retorno dos níveis de qualidade aceitável dos serviços de TI;

III. Os eventos não previstos na fase de planejamento do PCSTI e os procedimentos não documentados;

IV. Os valores dos parâmetros de RPO, RTO, WRT e MTD;

V. A eventual falta de recursos humanos ou tecnológicos;

VI. A eventual necessidade de desenvolvimento de competências.

Art. 23. Com base nas informações de monitoramento, o PCSTI deverá ser revisto a fim de adequá-lo às situações reais de ativação.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 24 São responsabilidades do CETI:

I. aprovar PCSTI de serviço crítico;

II. configurar e reconfigurar as designações dos responsáveis pela ativação e pelo gerenciamento de PCSTI de serviços críticos;

III. aprovar planos de teste de PCSTI de serviço críticos e respectivo cronograma;

Art. 25 São responsabilidades do Dirigentes da TI-PGT e da TI-Regional:

I. Manter atualizados os mapeamentos de serviços existentes, respeitada a diretriz de descontinuidade de padrões regionais e de promoção de padrões nacionais;

II. De forma coordenada, participar do planejamento, do desenvolvimento, dos testes, das implementações, do monitoramento, e da atualização dos PCSTI;

III. informar ao CETI sobre a situação dos PCSTI dos serviços críticos.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 26 A Assessoria de Segurança de TI da TI-PGT submeterá ao CETI, no prazo de 60 (sessenta) dias, o modelo de planejamento e de desenvolvimento dos PCSTI.

Art. 27 Os casos omissos serão resolvidos pelo CETI, em Nota Técnica, ouvidos os interessados.

Art. 28 Esta resolução entra em vigor na data de sua publicação.

Luis Fabiano de Assis
Procurador do Trabalho
Presidente do Comitê Estratégico de Tecnologia da Informação do MPT