TRIBUNAL REGIONAL ELEITORAL DO PARA

INSTRUÇÃO NORMATIVA Nº 11, DE 23 JUNHO DE 2025

Institui o Plano de Continuidade de Serviços de Tecnologia da Informação e Comunicação (PCSTI) no âmbito do Tribunal Regional Eleitoral do Pará e dá outras providências.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ , no uso de suas atribuições legais e regulamentares,

CONSIDERANDO:

I - A criticidade e a dependência dos serviços judiciais e administrativos do Tribunal em relação aos recursos de Tecnologia da Informação e Comunicação (TIC);

II - A necessidade de assegurar a disponibilidade e a resiliência dos serviços de TIC essenciais, minimizando o impacto de incidentes disruptivos nas operações do Tribunal, conforme preconiza a Resolução CNJ nº 370, de 28 de janeiro de 2021 (ENTIC-JUD);

III - A importância de estabelecer uma estrutura formal de governança para a gestão da continuidade, em alinhamento com a Resolução TRE/PA nº 5.419, de 2018, que institui a Política de Governança de TIC deste Tribunal;

IV - A identificação de ameaças e riscos com potencial de interrupção dos serviços, formalizada na Matriz de Riscos de TIC do TRE-PA;

V - A conclusão da elaboração do Plano de Continuidade de Serviços de TIC (PCSTI) pela Secretaria de Tecnologia da Informação, documento que detalha as estratégias, responsabilidades e procedimentos para a recuperação de serviços em caso de desastre;

VI - A necessidade de formalizar, regulamentar e dar publicidade ao PCSTI, estabelecendo sua observância por todas as unidades do Tribunal;

VII - O constante dos autos do Processo SEI nº 0005977-59.2025.6.14.8000;

RESOLVE:

Art. 1º Fica instituída a **Política de Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação** no âmbito do Tribunal Regional Eleitoral do Pará, cujas diretrizes são estabelecidas nesta Instrução Normativa.

Art. 2º Fica estabelecido o prazo máximo de 30 (trinta) dias, a contar da data de migração final de todos os ativos para o novo Data Center Modular, para a conclusão e aprovação, pelo Secretário de Tecnologia da Informação, do Plano Operacional de Continuidade de Serviços de TIC (PCSTI), considerando os processos e ativos críticos do Tribunal.

§1º O plano de continuidade de serviços de TI será preliminarmente avaliada pela Comissão de Segurança de Informação e aprovada e convalidade pelo Comitê Técnico de TI (CTTI).

§2º O plano será divulgado apenas em ambiente interno evitando exposição desnecessária de informações relativas à segurança do ambiente computacional.

Art. 3º São objetivos da Política e do Plano de Continuidade de Serviços de TIC:

I - Minimizar os impactos operacionais, financeiros e de imagem decorrentes de uma interrupção dos serviços de TIC;

II - Assegurar que os serviços críticos de TIC sejam recuperados dentro dos prazos definidos e aceitáveis para o negócio do Tribunal;

III - Estabelecer procedimentos e responsabilidades claras para a atuação das equipes em cenários de crise.

Art. 4º Esta Política é regida pelas seguintes diretrizes gerais:

I - A continuidade dos serviços de TIC é um componente essencial da governança de TI;

II - A definição da criticidade dos serviços deve ser baseada em uma Análise de Impacto no Negócio (BIA);

III - A análise de riscos de interrupção deve ser realizada e revisada periodicamente;

IV - O Plano de Continuidade (PCSTI) deve ser documentado, implementado e mantido;

V - O PCSTI deve ser testado e exercitado periodicamente;

VI - Deve ser designada uma equipe formal para gerenciar a continuidade dos serviços;

VII - Os procedimentos de comunicação durante uma crise devem ser claros e previamente estabelecidos.

CAPÍTULO II

DA GESTÃO DA CONTINUIDADE

Art. 5º A Análise de Impacto no Negócio (BIA) deverá ser conduzida e revisada periodicamente pela STI, em colaboração com as áreas de negócio, para identificar os serviços de TIC críticos e definir seus respectivos Objetivos de Tempo de Recuperação (RTO) e Objetivos de Ponto de Recuperação (RPO).

Art. 6º O Plano de Continuidade de Serviços de TIC (PCSTI), a ser concluído nos termos do Art. 2º, deverá detalhar, no mínimo:

I - As atribuições e responsabilidades das equipes de resposta;

II - Os critérios para acionamento do plano;

III - Os procedimentos de recuperação para cada serviço e ativo crítico;

IV - O plano de comunicação de crises.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 7º Compete à Secretaria de Tecnologia da Informação (STI), por meio de suas unidades e equipes designadas no PCSTI, manter, executar e testar o plano e seus procedimentos.

Art. 8º Compete à Equipe de Continuidade de TI (ECTI), coordenada pelo Coordenador de Continuidade de TI (CCTI), executar as ações de recuperação e gerenciamento da crise, conforme detalhado no PCSTI.

Art. 9º Compete aos gestores das demais unidades do Tribunal colaborar com a STI na identificação de seus processos de negócio críticos e na validação dos requisitos de continuidade.

CAPÍTULO IV

DAS DEFINIÇÕES

Art. 10. Para os fins e efeitos desta Instrução Normativa, adotam-se as seguintes definições:

I - **BIA (Business Impact Analysis):** Análise de Impacto no Negócio. Processo que identifica e avalia os potenciais efeitos de uma interrupção nos processos críticos de negócio.

II - **PCSTI:** Plano de Continuidade de Serviços Tecnologia da Informação e Comunicação.

III - **RTO (Recovery Time Objective):** Objetivo de Tempo de Recuperação. O período máximo de tempo que um sistema ou serviço pode ficar indisponível.

IV - **RPO (Recovery Point Objective):** Objetivo de Ponto de Recuperação. A quantidade máxima de perda de dados que pode ser tolerada, medida em tempo.

V - **DR (Disaster Recovery):** Recuperação de Desastres.

VI - **ECTI (Equipe de Continuidade de TI):** Grupo de pessoas com papéis e responsabilidades definidas para acionar, executar e supervisionar o PCTI.

VII - **CCTI (Coordenador de Continuidade de TI):** Responsável por coordenar a ECTI e as ações de continuidade.

VIII - **LET (Líder de Equipe Técnica):** Responsável por liderar as equipes técnicas durante a recuperação.

IX - **ETIR (Equipe de Tratamento e Resposta a Incidentes):** Equipe responsável pela gestão de incidentes de segurança da informação, exercida pela CGSI.

CAPÍTULO V

DAS PERDAS E INTERRUPÇÕES

Art. 11. O Objetivo de Tempo de Recuperação (RTO) fica definido em:

I – Sistemas críticos: até 48h.

II – Sistemas não-críticos: até 72h.

III – Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On): até 24h.

IV – Sistemas de homologação e testes: Sem tempo definido.

Art. 12. O Objetivo de Ponto de Recuperação (RPO) fica definido em:

I – Sistemas críticos: até 6h.

II – Sistemas não-críticos: até 24h.

III – Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On): 12h

Art. 13. O Período Máximo de Interrupção Tolerável (MTO) fica definido em:

I – Sistemas críticos: até 72h.

II – Sistemas não-críticos: até 168h.

III – Infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (Active Directory e Single-Sign-On), inclusive Links Internet: 12h.

IV – Sistemas de homologação e testes: Sem tempo definido.

CAPÍTULO VI

DOS TESTES E DA MANUTENÇÃO

Art. 14. O PCSTI, após sua aprovação, deverá ser submetido a testes periódicos, no mínimo anualmente, para validar sua eficácia e garantir o preparo das equipes. O resultado dos testes será documentado, encaminhado para a administração do TRE-PA no prazo máximo de 60(sessenta) dias, para posterior avaliação pela Comissão de Segurança da Informação, que poderá solicitar ajustes ou outras providências.

Art. 15. O PCSTI será revisado, no mínimo, a cada 2 (dois) anos ou sempre que ocorrerem mudanças significativas na infraestrutura, nos serviços críticos ou após os resultados de um teste indicarem a necessidade de melhorias.

Art. 16. O PCSTI e seus apêndices técnicos, por conterem informações sensíveis, são classificados como de acesso **Restrito**.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 17. Os casos omissos nesta Instrução Normativa serão dirimidos pelo Coordenador de Continuidade de TI (CCTI) em conjunto com a Comissão de Segurança da Informação

Art. 18. Esta Instrução Normativa entra em vigor na data de sua publicação.

Belém, 23 de junho de 2025.

Documento assinado eletronicamente por **BRUNO GIORGI ALMEIDA E SILVA**, **Diretor-Geral**, em 23/06/2025, às 22:38, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2732669** e o código CRC **DD0F978D**.