TRIBUNAL REGIONAL ELEITORAL DO ACRE

INSTRUÇÃO NORMATIVA Nº 37, DE 17 DEZEMBRO DE 2018

Estabelece diretrizes e define o processo de Gestão de Continuidade de Serviços Essenciais de Tecnologia da Informação, aplicáveis ao ambiente tecnológico deste Tribunal.

A PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ACRE, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de assegurar a disponibilidade das informações e prestação de serviços, como preconizado pela Resolução TRE-AC nº 1.716/2017, que estabelece a Política de Segurança da Informação da Justiça Eleitoral do Acre;

CONSIDERANDO a Norma Técnica ABNT NBR ISO/IEC 22313:2015, que fornece orientação para o planejamento, criação, implantação, operação, monitoramento, análise crítica, manutenção e melhoria contínua de um sistema de gestão documentado, que permite que as organizações se preparem para responder e recuperar-se de incidentes de interrupção quando eles surgirem.

CONSIDERANDO a necessidade de estabelecer procedimentos de gestão para assegurar a continuidade de serviços essenciais de TIC, especialmente no que se refere aos serviços judiciais, em atendimento à Resolução CNJ nº 211/2015.

R E S O L V E:

Art. 1º Esta norma, integrante da Política de Segurança da Informação do Tribunal Regional Eleitoral do Acre, estabelece as diretrizes e define o processo de Gestão de Continuidade de Serviços Essenciais de Tecnologia da Informação.

Art. 2º Para efeito desta Instrução Normativa, consideram-se:

1. atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

2. Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação jurisdicional do Tribunal, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

3. continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções dos negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

4. desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.

5. estratégia de continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior;

6. gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

7. plano de continuidade: nome que se dá à documentação que abrange os procedimentos referentes à continuidade dos serviços de TIC e é composta por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.

8. Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.

9. Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TIC, visando o retorno à normalidade.

10. resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

11. RPO (Recovery Point Objective): Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre.

12. RTO (Recovery Time Objective): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

DAS DIRETRIZES DA GESTÃO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TI

Art. 3º A gestão de continuidade de TI observará as seguintes diretrizes:

I. considerar o resultado da análise de riscos de TI e da análise de impacto de negócio realizadas, de forma a nortear a estratégia de continuidade dos serviços essenciais;

II. elaborar plano de continuidade de serviços essenciais de TI, com vistas ao registro dos procedimentos necessários à operação em nível de contingência e comunicações necessárias, bem como o retorno à normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TI;

III. alocar recursos humanos, tecnológicos e financeiros para a manutenção e melhoria da gestão de continuidade de serviços essenciais de TI;

IV. reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TI que suportam as atividades críticas do Tribunal;

V. manter os sistemas e serviços críticos de TI em nível minimamente operacional e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação de serviços no Tribunal;

VI. definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne à normalidade;

VII. proporcionar o correto direcionamento e dimensionamento de recursos tecnológicos para prover a gestão de continuidade de serviços essenciais de TI.

DO PROCESSO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TI

Art. 4º O processo de gestão de continuidade de serviços essenciais de TI é composto pelas seguintes etapas:

1. **planejamento** - compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades de TI são essenciais para o Tribunal, que serão tratadas na continuidade de serviços de TI, as estratégias que serão utilizadas durante eventuais incidentes e, ainda, a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças na infraestrutura, procedimentos ou testes realizados;

2. execução - abrange a elaboração, aprovação e revisão dos planos, com a descrição dos cenários de falhas e procedimentos técnicos para lidar com os problemas; a realização de testes (execução parcial ou integral dos procedimentos); armazenamento e divulgação;

3. verificação - abrange a realização de testes periódicos dos planos e a análise dos incidentes críticos ocorridos (desastres), a fim de subsidiar a etapa de melhoria;

4. melhoria - compreende a identificação das oportunidades de melhoria, com vistas a dar início a novo ciclo do processo.

Parágrafo único. O desenho do processo de gestão de continuidade de serviços essenciais de TI, a descrição das atividades, respectivos papéis e responsabilidades dos envolvidos, bem como os modelos de documentos e indicadores definidos serão publicados na intranet, após aprovação.

DO PLANO DE CONTINUIDADE DE SERVIÇOS ESSENCIAIS DE TI

Art. 5º O Plano de Continuidade de Serviços Essenciais de TI é composto pelos Planos de Continuidade Operacional e Planos de Recuperação de Desastres, devendo:

I. ser periodicamente testado, de forma a garantir sua efetividade.

II. ser revisado a cada dois anos, ou, ainda, em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades etc).

III. ser acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas do TRE-AC.

Art. 6º Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre, para retorno das atividades à normalidade.

Art. 7º A comunicação aos interessados observará as orientações contidas nos Planos de Continuidade Operacional.

Art. 8º Os ativos e serviços afetados pelo incidente serão monitorados pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações à autoridade superior.

Art. 9º A execução do Plano de Continuidade de Serviços Essenciais de TI será encerrada quando da comunicação de retorno à normalidade dos serviços, sistemas ou ativos afetados.

Art. 10. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Continuidade Serviços Essenciais de TI.

Art. 11. Esta Instrução Normativa entrará em vigor na data de sua publicação, devendo ser atualizada a cada 2 (dois) anos ou sempre que necessário.

Art. 12. Os casos omissos serão dirimidos pela Diretoria-Geral, ouvida a Comissão de Segurança da Informação.

Rio Branco, 17 de dezembro de 2018.

Documento assinado eletronicamente por **Regina Célia Ferrari Longuini**, **Presidente**, em 20/12/2018, às 11:18, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0252230** e o código CRC **564F386B**.