TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO

INSTRUÇÃO NORMATIVA Nº 18, DE 17 DE MAIO DE 2017

Estabelece diretrizes quanto à política de Continuidade de Negócios da Justiça Eleitoral de Pernambuco.

O **PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO**, no uso de suas atribuições, de conformidade com o disposto na Resolução nº 164, de 10 de julho de 2012, e considerando o Plano de Trabalho de 2016-2018, da Comissão de Segurança da Informação, o Acórdão - TCU nº 749/2014-Plenário, a Resolução - TSE nº 23.501, de 19 de dezembro de 2016, (Política de Segurança da Informação da Justiça Eleitoral - PSI) e a Resolução - CNJ nº 211, de 15 de dezembro de 2015, (Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário – ENTIC-JUD),

RESOLVE:

Art. 1º As diretrizes gerais para a Gestão da Continuidade de Negócios relativos aos processos críticos do TRE-PE obedecerão às regras estabelecidas no anexo desta instrução normativa.

Art. 2º Para composição da Gestão da Continuidade de Negócios, as unidades administrativas do TRE-PE devem desenvolver Planos de Continuidade dos Serviços estabelecidos como essenciais para cada unidade, em alinhamento com os processos críticos do Órgão.

Art. 3º As regras estabelecidas nesta instrução normativa devem ser implantadas gradativamente em até dezoito meses, a partir de sua publicação.

Art. 4º Esta instrução normativa entra em vigor na data de sua publicação.

Recife, 17 de maio de 2017.

Des. ANTONIO CARLOS ALVES DA SILVA
Presidente

INSTRUÇÃO NORMATIVA Nº XX/2017

ANEXO

1 - OBJETIVO

Desenvolver, estabelecer e manter o Plano de Continuidade de Negócios, que será composto pelos Planos de Continuidade de Serviços das unidades administrativas do TRE-PE, visando à manutenção ou recuperação dos serviços essenciais, em resposta a incidentes e interrupções, mantendo operacionais os processos críticos da Instituição.

1.1 - SEÇÕES CONTEMPLADAS NESTA INSTRUÇÃO NORMATIVA

SEÇÃO	NOME	OBJETIVO
S001-1	Definição da política, objetivos e escopo da continuidade de negócio.	Definir a política e o escopo de continuidade de negócio, alinhado aos objetivos, à gestão de riscos do TRE-PE e às partes interessadas.
S001-2	Desenvolvimento e implementação do plano de continuidade de negócio.	Desenvolver plano de continuidade de negócio (PCN) para a manutenção ou recuperação das operações críticas.
S001-3	Testes, manutenção e reavaliação dos planos de continuidade de negócio.	Testar os planos de continuidade de negócio e atualizá-los regularmente para assegurar a sua efetividade.
S001-4	Desenvolvimento de plano contínuo de treinamento para os envolvidos no PCN.	Prover treinamento regular sobre procedimentos, papéis e responsabilidades.

2 - DOCUMENTOS DE REFERÊNCIA

ABNT NBR 15999-1:2007: – Gestão de Continuidade de Negócios Parte 1: Código de prática.

Acórdão - TCU nº 749/2014 – Plenário, que trata do resultado da auditoria em governança de TI realizada no TRE-PE.

NBR/ISO/IEC 27002:2005 - Código de prática para gestão da Segurança da Informação.

COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização

Resolução - CNJ nº 211, de 15/12/2015, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

Resolução - TSE nº 23.501, de 19/12/2016, que Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

3 - DEFINIÇÕES

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançar os objetivos nas políticas [ISO/IEC 13335-1:2004].

Recurso de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura ou as instalações físicas que os abriguem [ABNT ISO/IEC 27002:2005].

Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação [ABNT ISO/IEC 27002:2005].

Política: intenções e diretrizes globais formalmente expressas pela direção [ABNT ISO/IEC 27002:2005].

Risco: combinação da probabilidade de um evento e de suas conseqüências [ABNT ISO/IEC Guia 73:2005].

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização [ISO/IEC 13335-1:2004].

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças [ABNT ISO/IEC 27002:2005].

Servidores: profissionais integrantes do quadro de lotação do TRE-PE.

Prestadores de Serviço: profissionais autônomos ou colaboradores pertencentes ao quadro funcional das empresas que realizam trabalhos para o TRE-PE.

Usuários: pessoas que acessam ou fazem uso de recursos ou sistemas de informação do TRE-PE.

4 - SEÇÃO S001-1: DEFINIÇÃO DA POLÍTICA, OBJETIVOS E ESCOPO DA CONTINUIDADE DE NEGÓCIO

Definir a política e o escopo de continuidade de negócio, alinhado aos

objetivos, à gestão de riscos do TRE-PE e às partes interessadas.

4.1 - Definições, Escopo e Partes Interessadas

4.1.1 - Considerando o Planejamento Estratégico Institucional – PEI, cada unidade administrativa deve identificar os processos de negócios críticos, terceirizados e os serviços essenciais a eles vinculados.

4.1.2 - O rol de serviços identificados como essenciais deve ser submetido ao COGEST para validação, momento em que será verificado o alinhamento com o PEI.

4.1.3 - Para cada serviço essencial validado devem ser identificadas as principais partes interessadas, bem como os responsáveis.

4.1.4 - Devem ser definidas, documentadas e validadas pelas partes interessadas as diretrizes mínimas para assegurar a continuidade dos serviços essenciais, bem como incorporadas à cultura da Instituição.

4.1.5 - Para definição das diretrizes, devem ser considerados:

4.1.5.1 - condições e procedimentos necessários à continuidade dos processos essenciais;

4.1.5.2 - cenários suscetíveis que possam causar incidentes significativos de interrupção;

4.1.5.3 - análise de impacto para os serviços essenciais frente à ocorrência dos cenários identificados;

4.1.5.4 - tempo máximo tolerável de paralisação dos serviços;

4.1.5.5 - tempo mínimo necessário para recuperação após incidente, observados os limites referidos no item anterior;

4.1.5.6 - tempo máximo admitido, antes de uma falha ou desastre, durante o qual as alterações feitas aos dados podem ser perdidas;

4.1.5.7 - probabilidade e impacto das ameaças que podem causar perda de continuidade, com identificação das medidas para sua prevenção e maior resiliência;

4.1.5.8 - recursos financeiros, organizacionais, técnicos e ambientais para cada opção estratégica e/ou técnica que vise à continuidade;

4.1.5.9 - requisitos de segurança de pessoal e proteção de recursos de processamentos das informações e bens da Instituição;

4.1.5.10 - Plano de Gestão de Riscos instituído pela Resolução - TRE-PE nº 277/2016.

4.1.6 - As diretrizes definidas para cada serviço essencial, visando à manutenção da continuidade do negócio, devem ser submetidas ao COGEST.

5 - SEÇÃO S001-2: DESENVOLVIMENTO E IMPLEMENTAÇÃO DE PLANOS DE CONTINUIDADE DE NEGÓCIO

Objetiva desenvolver e implementar planos para a manutenção ou recuperação das operações e para assegurar a disponibilidade dos serviços críticos.

5.1 - Procedimentos e Ações

5.1.1 - Devem ser descritas as ações que serão colocadas em prática para permitir a recuperação e restauração das operações críticas.

5.1.2 - Devem ser descritas, quando houver, as dependências externas e/ou a contratos vigentes.

5.1.3 - Os planos devem ser validados pelas partes interessadas.

5.1.4 - Para elaboração dos planos, devem ser descritos:

5.1.4.1 - papéis e responsáveis pelos planos de continuidade, incluindo os procedimentos a serem adotados quando da decisão, as pessoas que devem ser consultadas antes da decisão e as pessoas que devem ser informadas da decisão;

5.1.4.2 - procedimentos e ações de todos os envolvidos na execução do plano;

5.1.4.3 - recursos necessários à execução dos procedimentos e ações, tais como pessoas, instalações e infraestrutura;

5.1.4.4 - procedimentos de atualização e reconciliação das informações, inclusive dos bancos de dados envolvidos;

5.1.4.5 - requisitos de *backup* necessários para suportar o plano, tais como: dados a serem salvaguardados, período de retenção desses dados e tempo aceitável de perda de dados após desastre (RPO);

5.1.4.6 - habilidades e conhecimento necessários para os envolvidos na execução do plano;

5.1.4.7 - procedimentos e ações sob responsabilidade de prestadores de serviços terceirizados;

5.1.4.8 - contatos atualizados dos agentes internos ou externos que possam ser necessários à retomada dos serviços.

5.1.5 - Os planos elaborados para cada serviço essencial, visando à manutenção da continuidade do negócio, devem ser submetidos ao COGEST.

5.1.6 - Devem ser mantidas cópias dos planos de continuidade de negócio em ambiente remoto, à distância suficiente para permanecerem preservados no caso de dano ou desastre no local principal.

5.1.7 - Os planos de continuidade de negócio devem ser amplamente divulgados por cada unidade responsável com auxílio da ASCOM.

6 - SEÇÃO S001-3: TESTES, MANUTENÇÃO E REAVALIAÇÃO DOS PLANOS DE CONTINUIDADE DO NEGÓCIO

Objetiva testar os planos de continuidade do negócio e atualizá-los regularmente para assegurar a sua efetividade.

6.1 - Testes

6.1.1 - Devem ser definidos objetivos para testes dos recursos e sistemas de negócio, técnicos, administrativos, processuais e operacionais visando atestar a completude dos planos.

6.1.2 - Devem ser elaborados testes realistas com as partes interessadas, visando validar os procedimentos de continuidade e identificar melhorias objetivando a mínima interrupção dos processos de negócio essenciais.

6.1.3 - Devem ser atribuídas responsabilidades para a realização dos testes e exercício dos planos de continuidade, inclusive aquelas referentes a prestadores de serviços terceirizados, quando for necessário.

6.1.4 - Devem ser estabelecidos cronogramas formais para realização dos testes.

6.1.5 - Deve ser realizada e documentada reunião de análise pós-teste para avaliar os resultados e recomendar oportunidades de melhoria.

6.1.6 - O relatório produzido após a realização dos testes deve ser assinado por todos os envolvidos, inclusive pelas partes interessadas.

6.2 - Manutenção

6.2.1 - Os planos de continuidade devem ser revistos:

6.2.1.1 - após a realização de testes, considerando os atuais objetivos operacionais e estratégicos;

6.2.1.2 - na ocorrência de mudanças que tenham impacto nos serviços essenciais, tais como pessoal, estratégia de negócio, localização, instalações e recursos, legislação, fornecedores, processos e riscos;

6.2.1.3 - após a aplicação do plano de continuidade de negócio em decorrência de uma interrupção, verificando a aderência ao plano, sua eficácia, recursos necessários, papéis e responsabilidades, habilidades e competências, resiliência ao incidente, infraestrutura técnica e as estruturas organizacionais.

6.2.2 - Devem ser identificadas, pelas unidades responsáveis, as deficiências ou omissões no plano para indicação das recomendações de melhoria.

6.2.3 - Os planos revisados, visando à manutenção da continuidade do negócio, devem ser submetidos ao COGEST.

6.2.4 - Devem ser comunicadas, pelas unidades responsáveis, as alterações na política, planos, procedimentos, infraestrutura e papéis e responsabilidades.

7 - SEÇÃO S001-4: DESENVOLVIMENTO DE UM PLANO CONTÍNUO DE TREINAMENTO

Objetiva prover treinamento regular sobre procedimentos, papéis e responsabilidades.

7.1 - Plano Contínuo de Treinamento

7.1.1 - Devem ser definidos requisitos técnicos e gerenciais necessários ao planejamento, elaboração, aplicação e avaliação dos planos de continuidade.

7.1.2 - A partir da avaliação das partes interessadas envolvidas nos Planos de Continuidade, devem ser desenvolvidas competências com base em formação prática, incluindo participação em testes e exercícios.

7.1.3 - Devem ser monitoradas as habilidades e competências com base nos resultados dos exercícios e testes, visando a continua atualização do plano de capacitação.

7.1.4 - Os treinamentos necessários à implantação, execução e atualização do Plano de Continuidade de Negócios devem constar no Plano de Capacitação Institucional.