



TRIBUNAL REGIONAL ELEITORAL DO ACRE

INSTRUÇÃO NORMATIVA Nº 35, DE 03 AGOSTO DE 2018

Institui a Política de *Backup* de informações no âmbito do Tribunal Regional Eleitoral do Acre.

A DESEMBARGADORA REGINA CÉLIA FERRARI LONGUINI, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO ACRE, no uso de suas atribuições legais e regimentais,

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

CONSIDERANDO que a perda de informações pode significar dificuldades administrativas e até a paralisação de atividades essenciais do Tribunal;

CONSIDERANDO, por fim, o disposto na Resolução CNJ nº 211/2015, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD),

R E S O L V E:

DAS DISPOSIÇÕES GERAIS

Art. 1º Esta norma, integrante da Política de Segurança da Informação do Tribunal Regional Eleitoral do Acre, institui a Política de *Backup* das informações no âmbito deste Regional, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação, visando a garantir a sua integridade e disponibilidade.

Parágrafo único. O mero procedimento de *backup* não pode ser confundido ou utilizado como uma estratégia de temporalidade e sim para a recuperação de desastres, perda de dados originais por apagamentos acidentais ou corrupção de dados.

Art. 2º Para o disposto nesta portaria, considera-se:

I – *administrador de backup*: servidor responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e *restore*;

II - *backup*: cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais;

III – *backup full ou completo*: modalidade de *backup* na qual todos os dados são copiados;

IV - *backup incremental*: modalidade de *backup* na qual somente os arquivos modificados desde o último *backup* são copiados;

V - *gestor de ativo de informação*: proprietário ou custodiante de ativo de informação;

VI – *log*: histórico de avisos, erros e mensagens de aplicativos e sistemas;

VII – *mídia*: meio físico no qual se efetivamente armazena o *backup*;

VIII – *Restore*: recuperação dos arquivos existentes em um *backup*;

IX – *retenção*: período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;

X – *RTO - Recovery Time Objective (Tempo Objetivado de Recuperação)*: período de tempo após um incidente em que o produto, serviço ou atividade devem ser retomados;

XI – *RPO – Recovery Point Objective (Ponto Objetivado de Recuperação)*: ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

Art. 3º Os administradores de *backup* serão os servidores lotados na unidade da Secretaria de Tecnologia da Informação designada para esta função no Regimento Interno da Secretaria.

Art. 4º São atribuições dos administradores de *backup*:

I - propor modificações visando ao aperfeiçoamento da política de *backup*;

II - criar e manter os *backups*;

III - configurar a ferramenta de *backup*, com, no mínimo, periodicidade, conteúdo e relatórios;

IV - preservar as mídias de *backup*;

V - testar os procedimentos de *backup* e *restore*;

VI - executar procedimentos de *restore*;

VII - gerenciar mensagens e *logs* diários dos *backups*, através dos relatórios, fazendo o tratamento dos erros de forma que o procedimento de *backup* tenha sequência e os erros na sua execução sejam eliminados;

VIII - realizar manutenções periódicas dos dispositivos de *backup*;

IX - comunicar o gestor sobre os erros e ocorrências nos *backups* dos ativos de informação sob sua responsabilidade;

X – reportar ao superior hierárquico o resultado da execução e dos testes dos procedimentos de *backup* e *restore*;

XI - documentar os procedimentos previstos nos incisos II a IX deste artigo;

XII - registrar a execução dos procedimentos elencados neste artigo, visando à manutenção de histórico de ocorrências.

DO PROCEDIMENTO DE *BACKUP*

Art. 5º Todo e qualquer ativo de informação deverá ter sua inclusão nos procedimentos de *backup* avaliada.

§ 1º O gestor de cada ativo de informação, em conjunto com os administradores de *backup*, deverá definir, através de formulário, o que será incluído no *backup* e quais os tempos de restauração (indisponibilidade), retenção e perda de dados aceitáveis.

§ 2º A definição dos *backups* e demais informações técnicas deverão constar em uma planilha denominada “Estratégia de Execução de *Backup*”, publicada na *Intranet* e em processo eletrônico relacionado (SEI), que deverá ser atualizada pela equipe de administração de *backup* sempre que houver demanda, observado o disposto no parágrafo anterior.

§ 3º A planilha descrita no item anterior, contendo a situação atual, é parte integrante desta norma (Anexo I).

Art. 6º Os arquivos de dados institucionais deverão ser armazenados nos servidores de arquivos correspondentes e serão incluídos na rotina *backup*, obedecendo o disposto no artigo anterior.

Parágrafo único. Os dados armazenados nas estações de trabalho, bem como os inseridos nas pastas compartilhadas destinadas à transferência temporária, são de responsabilidade única e exclusiva do usuário, não sendo incluídos nas rotinas de *backup*.

Art. 7º A criação e operação de *backups* deverá obedecer às seguintes diretrizes:

I - o *backup* deverá ser programado, preferencialmente, para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede;

II - os administradores de *backups* deverão certificar-se da conclusão bem sucedida destes, analisando, se for o caso, os arquivos de *log*, para garantir o resultado da operação;

III – em caso de problemas na operação de *backups*, as causas deverão ser analisadas, reparadas e, quando necessário, um novo *backup* deverá ser imediatamente realizado;

IV – as mídias utilizadas no processo de realização do *backup* deverão possuir identificação suficiente para permitir, direta ou indiretamente, a localização e extração das informações nelas armazenadas;

V - todo *backup* efetuado deverá ser armazenado em pelo menos duas cópias em locais fisicamente distintos que possuam os requisitos de segurança adequados;

VI – a Administração do Tribunal deverá garantir que o parque de equipamentos servidores sejam suficientes para permitir a restauração dos *backups* em equipamentos distintos do original.

Art. 8º O *backup* dos sistemas eleitorais e de seus arquivos de banco de dados serão realizados conforme orientações do Tribunal Superior Eleitoral.

DO PROCEDIMENTO DE *RESTORE*

Art. 9º O procedimento de *restore* deverá obedecer o seguinte:

I - o gestor de ativo de informação que precise recuperar informações deverá solicitar formalmente, justificando o motivo da solicitação;

II - esta solicitação será encaminhada aos administradores de *backup* para que realizem a recuperação e comuniquem o resultado do procedimento.

Parágrafo único. É vedado o *restore* diretamente sobre os ambientes de produção, exceto em situações de recuperação de desastre ou plano de contingência.

DOS TESTES DE *BACKUP* E *RESTORE*

Art. 10. Os procedimentos de *backup* e *restore* deverão ser testados, por amostragem, no mínimo trimestralmente ou sempre que necessário.

Parágrafo único: os resultados dos testes de *backup* e *restore* deverão ser comunicados à Coordenadoria de Infraestrutura.

DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE *BACKUP*

Art. 11. Os administradores de *backup* deverão respeitar os critérios definidos pelos fabricantes para assegurar a validade e a qualidade das mídias utilizadas na realização de *backups*.

Art. 12. No caso de substituição da solução utilizada nos *backups*, as informações contidas nas mídias da antiga solução deverão ser transferidas em sua totalidade para as mídias da nova solução.

Art. 13. O descarte das mídias utilizadas para *backup* deve ser realizado de forma a impossibilitar a recuperação total ou parcial das informações.

DISPOSIÇÕES FINAIS

Art. 14. A execução de quaisquer procedimentos que impliquem riscos de funcionamento nos ativos de informação deverá ser precedida da realização de *backup*.

Art. 15. A revisão desta política de *backup* ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período máximo de 3 (três) anos.

Rio Branco, 03 de agosto de 2018.



Documento assinado eletronicamente por **Regina Célia Ferrari Longuini, Presidente**, em 08/08/2018, às 15:42, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site http://sei.tre-ac.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0224384** e o código CRC **1EE173FE**.