



PODER JUDICIÁRIO
TRIBUNAL REGIONAL ELEITORAL

PROCESSO ADMINISTRATIVO (1298) - 0600171-10.2021.6.02.0000 - Maceió - ALAGOAS

RESOLUÇÃO Nº 16.164
(26/10/ 2021)

Regulamenta a Política de Backup no âmbito do Tribunal Regional Eleitoral de Alagoas.

O TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS, no exercício de suas atribuições legais e regimentais,

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018, que instituiu a Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a Resolução CNJ nº 370, de 28 de janeiro de 2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução TSE nº 23.644, de 1º de julho de 2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO Resolução TRE/AL nº 15.732/2016, de 13 de setembro de 2016, que Dispõe sobre a Governança Corporativa de Tecnologia da Informação e Comunicação (TIC) no âmbito do Tribunal Regional Eleitoral de Alagoas e dá outras providências;

CONSIDERANDO o disposto no Processo SEI nº 0006643-35.2021.6.02.8000,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Backup no âmbito do Tribunal Regional Eleitoral de Alagoas, que fixa as diretrizes para a garantia da integridade e disponibilidade das informações no caso de necessidade de recuperação de dados perdidos ou excluídos.

Art. 2º Para efeito desta norma, compreende-se:

I - ativo de informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas (norma ABNT NBR ISO/IEC 27002);

II - administrador de backup: unidade responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;

III - backup: cópia de segurança que se faz regularmente, ou sob demanda, para assegurar que um arquivo ou o conjunto de dados de um dispositivo não se perca, sendo usado quando há prejuízo ou dano no arquivo original;

IV - gestor de sistema informatizado: responsável pelas regras de negócio de um sistema de informação, e que tem autonomia de decisão sobre os processos de trabalho abrangidos pelo sistema informatizado;

V - DR: Disaster Recovery (Recuperação de desastres) - finalidade de backups tipo imagem e de curto período de retenção;

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

VII - mídia: meio físico e/ou virtual no qual efetivamente se armazena o backup;

VIII - restore: recuperação dos arquivos ou conjunto de dados existentes em um backup;

IX - retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado.

Art. 3º As Coordenadorias de Infraestrutura (COINF) e de Soluções Corporativas (CSCOR) serão as unidades responsáveis pela administração dos procedimentos relativos aos serviços de backup e restore e guarda dos dados pelo período de retenção determinado, cada qual de acordo com seu escopo de atuação.

Art. 4º São atribuições da unidade administradora de backup:

I - propor o aperfeiçoamento da política de backup;

II - elaborar e manter o plano de backup, submetendo-o ao Comitê de Gestão de Tecnologia da Informação e Comunicação (CGTIC) para encaminhamento e aprovação por parte do Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC);

III - realizar e manter os backups;

IV - configurar a ferramenta de backup, abrangendo, no mínimo, periodicidade, conteúdo e relatórios;

V - preservar as mídias de backup;

VI - testar os procedimentos de backup e restore;

VII - executar procedimentos de restore;

VIII - monitorar mensagens e logs dos backups por meio de relatórios, realizando o tratamento dos erros, visando ao prosseguimento do backup e à eliminação dos erros;

IX - realizar manutenções periódicas dos dispositivos de backup;

X - comunicar os erros e as ocorrências nos backups ao gestor do sistema informatizado;

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

XII - registrar e manter histórico dos procedimentos de backup, restore, erros e ocorrências.

Art. 5º Os arquivos e dados armazenados nas estações de trabalho são de responsabilidade única e exclusiva do usuário ou usuária, que poderá solicitar orientações à COINF e CSCOR, conforme o caso, quanto aos procedimentos de backup e restore, via abertura de chamado.

CAPÍTULO II

PROCEDIMENTO DE BACKUP

Art. 6º Todo e qualquer ativo de informação que esteja registrado em equipamentos servidores do Centro de Processamento de Dados (CPD) será incluído nos procedimentos de backup.

Parágrafo único. O gestor ou gestora de sistema informatizado, em conjunto com a unidade administradora de backup, poderá definir periodicidade mínima e/ou tempo de retenção distinto dos estabelecidos nesta norma, desde que haja justificativa, recursos tecnológicos disponíveis e prévia autorização da Diretoria-Geral.

Art. 7º Os procedimentos de backup serão atualizados sempre que houver alterações nos requisitos dos dados dos ativos de informação e/ou novos recursos tecnológicos disponíveis.

Parágrafo único. As atualizações serão apresentadas pela unidade administradora de backup, por meio de Nota Técnica, submetidas ao Comitê de Gestão de TIC.

Art. 8º Os procedimentos de backup observarão as seguintes diretrizes:

I - Quanto ao tipo, os backups poderão ser:

- a) backup DR (Disaster Recovery) - imagem (cópia) fiel de toda a máquina;
- b) backup histórico - backup de arquivos e/ou imagens (DR) com período de retenção maior.

II - Para equipamentos servidores classificados como de Produção, Desenvolvimento e Homologação (virtuais e físicos):

- a) backup do tipo DR;

b) backup com periodicidade diária.

III - Para equipamentos servidores classificados como Banco de Dados de Produção:

a) backup do tipo DR, com periodicidade diária;

b) backup do tipo histórico de arquivos com periodicidade mensal.

IV - Para equipamentos servidores classificados como Banco de Dados de Desenvolvimento e Homologação:

a) backup do tipo DR;

b) backup com periodicidade semanal.

§ 1º O backup deverá ser programado para execução automática, em horários de menor ou nenhuma utilização dos sistemas e da rede de dados.

§ 2º A unidade administradora de backup deverá certificar-se do resultado das operações de backup, analisando, se for o caso, os arquivos de log.

§ 3º Em caso de problemas na operação de backups, as causas deverão ser analisadas, reparadas e, quando necessário, um novo backup deverá ser imediatamente reagendado.

§ 4º As mídias utilizadas no processo de realização de backup deverão possuir identificação suficiente para permitir, direta ou indiretamente, a localização e extração das informações nelas armazenadas.

§ 5º Os backups deverão ser armazenados, no mínimo, em duas cópias, em mídias e locais fisicamente distintos que possuam os requisitos de segurança adequados, admitidas exceções em razão do volume e criticidade dos dados, devidamente autorizadas pelo gestor ou gestora do sistema informatizado.

§ 6º A relação de dados a serem gravados em cada tipo de cópia, frequência de realização, descrição das mídias envolvidas e procedimentos de contingência a serem adotados em caso de falha deverá ser registrada e mantida pela unidade administradora de backup.

§ 7º O backup dos sistemas eleitorais e de seus arquivos de banco de dados serão realizados de acordo com as orientações do Tribunal Superior Eleitoral (TSE).

§ 8º A Classificação dos equipamentos cabe ao gestor de sistema informatizado auxiliado pela unidade administradora de backup e deve ser formalizada pelo primeiro.

Art. 9º A retenção dos backups observará os seguintes prazos:

I - backup diário: 5 dias;

II - backup semanal: 5 semanas;

III - backup mensal: 12 meses.

Parágrafo Único. A retenção poderá ser reduzida em caso de ausência ou falha dos equipamentos, mídias e/ou softwares necessários, desde que validado pela unidade administradora do backup.

CAPÍTULO III

PROCEDIMENTO DE RESTORE

Art. 10. O procedimento de restore será realizado pela unidade administradora de backup, mediante solicitação formal e justificada da área gestora do sistema informatizado ou da unidade administrativa responsável pela informação.

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

Art. 11. O tempo para realização do procedimento de restore será estimado pela unidade administradora de backup, em até 03 (três) dias úteis, ou, emergências em até 03 (três) horas após o recebimento da solicitação, oportunidade em que serão consideradas as variáveis envolvidas e a complexidade da operação.

CAPÍTULO IV

TESTES DE BACKUP E DE RESTORE

Art. 12. Os procedimentos de backup e restore deverão ser testados sempre que necessário, em período não superior a 12 meses.

CAPÍTULO V

DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE BACKUP

Art. 13. A unidade administradora de backup deverá respeitar os critérios definidos pelos fabricantes para assegurar a validade e a qualidade das mídias utilizadas na realização de backups.

Art. 14. Quando houver a substituição da solução utilizada na realização dos backups, as informações contidas nas mídias da antiga solução, que forem incompatíveis com a nova, deverão ser transferidas em sua totalidade para as mídias da nova solução.

Parágrafo único. A solução antiga somente poderá ser totalmente desativada após a confirmação de que todas as informações foram transferidas para a nova solução.

Art. 15. O descarte das mídias utilizadas para backup deverá ser realizado de forma a impossibilitar a recuperação total ou parcial das informações e obedecerá aos preceitos de destinação socioambiental, sendo, no contexto do art. 5º, o usuário, responsável direto.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 16. A execução de quaisquer procedimentos que impliquem em risco ao funcionamento dos ativos de informação deverá ser precedida da realização de backup, cabendo ao gestor de sistema informatizado, conforme o caso, a avaliação e autorização para a execução.

Art. 17. A revisão desta política de backup será realizada a cada 2 (dois) anos ou, quando necessário, em menor prazo.

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

Sala de Sessões do Tribunal Regional Eleitoral de Alagoas, em Maceió/AL, aos 26 dias do mês de outubro de 2021.

Des. OTÁVIO LEÃO PRAXEDES

Presidente

