

PORTARIA PRESIDÊNCIA N.º 256/2019 TRE/PRE/ASJES - INSTITUI A POLÍTICA DE BACKUP E RESTORE DAS INFORMAÇÕES NO ÂMBITO DO TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL.

O Desembargador DIVONCIR SCHREINER MARAN, PRESIDENTE DO EGRÉGIO TRIBUNAL REGIONAL ELEITORAL DO ESTADO DO MATO GROSSO DO SUL EM EXERCÍCIO, no uso das atribuições que lhe são conferidas pelo art. 22, inciso VI, do Regimento Interno do Tribunal (Resolução TRE/MS n.º 170/1997), e

Considerando a necessidade de assegurar a integridade e a disponibilidade das informações, como preconizado pela resolução TSE nº 23.501/2016, que estabelece a Política de Segurança da Informação da Justiça Eleitoral;

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

RESOLVE:

Art. 1º Instituir a política de *backup* e *restore* 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 (STI), visando garantir a sua integridade e disponibilidade, bem como o manual do processo de *backup* e *restore*, constante do Anexo único desta Portaria.

Parágrafo único. O mero procedimento de *backup* não pode ser confundido ou utilizado como uma estratégia de temporalidade – guarda ou preservação de longo prazo – e sim para a recuperação de desastres, perda de dados originais por acidente ou corrupção de dados.

DAS DISPOSIÇÕES INICIAIS

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 – Ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

III – *Backup*: cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais;

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

V – *Backup* incremental: modalidade de *backup* na qual somente os arquivos modificados desde o último *backup* são copiados;

VI – Gestor de ativo de informação: proprietário ou custodiante de ativo de informação;

VII – *Log*: histórico de avisos, erros e mensagens de aplicativos e sistemas;

VIII – Mídia: meio físico no qual se efetivamente armazena o *backup*;

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

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

Art. 3º A Seção de Suporte Operacional será responsável pelos procedimentos relativos aos serviços de *backup* e *restore*.

Art. 4º São atribuições da Seção de Suporte Operacional e dos administradores de *backup*:

I - propor modificações visando o 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 - documentar os procedimentos dos incisos II a IX deste artigo;

XI - registrar a execução dos procedimentos elencados neste artigo, visando a manutenção de histórico de ocorrências;

XII - identificar o tipo de *backup* a ser adotado no plano de *backup* (diário, semanal, mensal e/ou anual).

DO PROCEDIMENTO DE BACKUP

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

Parágrafo único. 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*.

Art. 6º Os arquivos de dados armazenados nas estações de trabalho são de responsabilidade única e exclusiva do usuário, que contará com orientações fornecidas pela STI de como proceder com procedimentos de *backup* e *restore*.

Art. 7º Os procedimentos de *backup* deverão ser atualizados sempre que houver alterações nos ativos de informação.

Art. 8º A retenção dos *backups* deverá observar os seguintes prazos:

I - no caso de *backup* diário: quinze últimos dias;

II - no caso de *backup* semanal: oito últimas semanas;

III - no caso de *backup* mensal: doze últimos meses;

IV - no caso de *backup* anual: cinco últimos anos.

§ 1º Em casos especiais, o gestor do ativo de informação poderá definir, em conjunto com os administradores de *backup*, prazos diferenciados para retenção dos *backups*.

§ 2º Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

Art. 9º A criação e operação de *backups* deverá obedecer às seguintes diretrizes:

I - o *backup* deverá ser programado 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 *backup*, 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 mídias diferentes e em locais fisicamente distintos que possuam os requisitos de segurança adequados.

Art. 10 O *backup* deverá ser realizado como disposto a seguir:

I - os *backups* semanais, mensais e anuais, se houverem, deverão ser realizados, preferencialmente, na modalidade *full*, de forma a poderem recuperar integralmente todas as informações sem a necessidade de outros *backups*.

II - o *backup* semanal, se houver, ocorrerá, preferencialmente, na sexta-feira, referindo-se à semana que se encerra.

III - o *backup* mensal, se houver, ocorrerá, preferencialmente, no primeiro dia de cada mês, referindo-se ao mês anterior.

IV - em caso de falha em algum procedimento de *backup* ou impossibilidade da sua execução, os administradores de *backup* deverão adotar as providências no sentido de salvaguardar as informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor ou execução do *backup* em horário de produção.

V - o *backup* do banco de dados Oracle deverá ser realizado, pelo menos, quatro vezes ao dia, na modalidade incremental, para reduzir a perda de transações.

Art. 11 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. 12 O procedimento de *restore* deverá obedecer o seguinte processo:

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. 13 Os procedimentos de *backup* e *restore* deverão ser testados sempre que necessário.

Art. 14 Os *backups* mensais e anuais deverão ser testados no prazo máximo de uma semana após a sua execução e, caso seja detectada falha no *backup* ou se o mesmo estiver incompleto, novo *backup* deverá ser executado com vistas ao seu armazenamento.

Art. 15 Os *backups* mensais e anuais deverão ser testados regularmente a fim de verificar a integridade da mídia.

DESCARTE E SUBSTITUIÇÃO DAS MÍDIAS DE *BACKUP*

Art. 16 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. 17 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.

Parágrafo Único. A solução antiga somente poderá ser completamente desativada após a confirmação, através de teste de *restore*, de que todas as informações foram transferidas para a nova solução implementada.

Art. 18 O descarte das mídias utilizadas para *backup* deve ser realizado de forma a impossibilitar a recuperação total ou parcial das informações.

DISPOSIÇÕES FINAIS

Art. 19 A execução de quaisquer procedimentos que impliquem riscos de funcionamento nos ativos de informação deverá ser precedida da realização de *backup*.

Art. 20 O estabelecido nesta norma é de uso obrigatório.

Art. 21 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.

Art. 22 Esta Portaria entra em vigor na data da assinatura.

Campo Grande (MS), na data da assinatura digital.

Desembargador DIVONCIR SCHREINER MARAN

Presidente em substituição

[REDACTED]