

Art. 27. O descumprimento desta instrução normativa deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.

Art. 28. Os casos omissos serão resolvidos pela CSI.

Art. 29. Esta instrução normativa entra em vigor na data de sua publicação.

Mário Lobão Carvalho

Diretor-Geral

## PORTARIAS

### **PORTARIA DG Nº 101/2023 TRE-MA/PR/DG/STIC ATUALIZA A POLÍTICA DE BACKUP E RESTORE DE DADOS NO ÂMBITO DESTE REGIONAL, COM O OBJETIVO DE ESTABELECEER DIRETRIZES PARA O PROCESSO DE CÓPIA E ARMAZENAMENTO DOS DADOS.**

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, no uso das atribuições que lhe são conferidas pelo art. 49 do Regulamento Interno da Secretaria deste Tribunal,

CONSIDERANDO o disposto na Resolução nº 370 do Conselho Nacional de Justiça, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD),

CONSIDERANDO a necessidade de garantir a disponibilidade dos dados e dos sistemas de informação,

CONSIDERANDO a necessidade de definir processos para a realização de cópias de segurança de dados e sistemas de informação administrados e armazenados no TRE-MA,

CONSIDERANDO que a segurança da informação é condição essencial para a prestação de serviços jurisdicionais e administrativos do TRE-MA,

RESOLVE:

Art. 1º Atualizar a Política de Backup e Restore de Dados no âmbito deste Regional, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados, visando garantir a sua integridade e disponibilidade.

Art. 2º Para o disposto nesta Portaria considera-se:

I - administrador de backup: é a unidade responsável pelos procedimentos de configuração, execução e monitoramento de backup e pelo acompanhamento dos testes nos procedimentos de restore;

II - administrador de recurso: é a unidade responsável pela operação de serviços ou equipamentos de TIC, bem como pela realização dos testes de restore;

III - backup: cópia de segurança de dados computacionais;

IV - backup full: backup em que todos os dados são copiados integralmente (cópia de segurança completa);

V - backup incremental: backup em que somente os arquivos novos ou modificados desde o último backup completo são copiados;

VI - clientes de backup: todo equipamento servidor no qual é instalada a ferramenta de backup;

VII - disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

VIII - integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

IX - mídia: meio físico no qual se armazenam os dados de um backup;

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

XI - restore: restauração de arquivos computacionais;

XII - replicação de backup: cópia de segurança realizada a partir do backup original, podendo ser armazenada em outro datacenter ou na nuvem.

Art. 3º Não estão cobertos por esta política os dados armazenados em microcomputadores, notebooks e dispositivos móveis, para os quais eventuais cópias de segurança são de responsabilidade do usuário.

Art. 4º A Seção de Gestão de Redes (SERED) será o administrador de backup, responsável pela elaboração de política e procedimentos relativos aos servidores de backup, de acordo com as normas aplicáveis.

Art. 5º É atribuição do administrador de backup:

I - providenciar a criação e manutenção dos backups;

II - configurar a ferramenta de backup;

III - supervisionar manutenções periódicas dos dispositivos de backup;

IV - efetuar testes de backup e auxiliar nos procedimentos de restore;

V - verificar diariamente os eventos gerados pela ferramenta de backup, tomando as providências necessárias para remediação de falhas;

VI - restaurar os backups em caso de necessidade;

VII - gerenciar mensagens e logs dos backups;

VIII - comunicar ao administrador de recurso os erros e as ocorrências nos backups; e

IX - propor modificações visando o aperfeiçoamento da política de backup.

Parágrafo único. O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

Art. 6º É atribuição do administrador de recurso:

I - solicitar a inclusão do recurso nas rotinas de backup e restore fornecendo as informações relativas ao backup, como servidor e dados a serem incluídos;

II - dar permissão ao administrador de backup para configurar e modificar a ferramenta cliente de backup no servidor;

III - validar o resultado do restore.

Art. 7º A criação e a operação dos backups deverão obedecer às seguintes orientações:

I - criação de backups:

a) o backup deverá ser criado na ferramenta de backup, seguindo as orientações conforme solicitado pelo administrador de recurso;

b) o backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede, conforme definição do administrador de backup em conjunto com o administrador de recurso.

II - operação de backups:

a) o backup deverá ser operado e monitorado pelo administrador de backup;

b) para cada backup realizado, deve ser gerado relatório automatizado pela própria ferramenta de backup, confirmando a execução da operação;

c) em caso de problemas na operação de backup, as causas deverão ser analisadas, reparadas e, quando necessário, um novo backup deverá ser imediatamente realizado.

Art. 8º A configuração e a monitoração das funcionalidades relativas ao banco de dados serão de responsabilidade do administrador do recurso.

Art. 9º Os backups deverão seguir políticas diferenciadas de acordo com o tipo de dado e o ambiente computacional, como disposto a seguir:

I - quanto ao método de backup:

a) Backup em Disco: Para rápida recuperação de dados e performance otimizada, os backups serão realizados inicialmente em disco. Este é o método principal de backup e recuperação.

b) Backup em Fita: Para a segurança de longo prazo e a proteção contra falhas de disco ou desastres naturais, os backups em disco serão copiados para fitas magnéticas. As fitas serão armazenadas em um local seguro fora do local de realização dos backups.

c) Backup na Nuvem: Para maior redundância e proteção contra falhas físicas, o TRE-MA também manterá uma cópia dos dados na nuvem para todos os backups realizados em disco.

II - quanto ao período de realização do backup:

a) diário: deverá ser programado para execução no intervalo entre às 20h e às 5h do dia seguinte, de segunda a sexta;

b) semanal: deverá ser programado para execução no intervalo entre às 20h de sábado e às 12h do domingo;

c) mensal: deverá ser programado para execução no intervalo entre às 20h do último dia do mês e às 5h do dia seguinte.

III - quanto à aplicação e retenção do backup realizado em disco:

a) em ambiente de produção:

a1) proveniente de servidor de arquivos: diário, com retenção de 14 dias; semanal, com retenção de 8 semanas; e mensal, com retenção de 12 meses;

a2) proveniente de servidor de aplicação: diário, com retenção de 7 dias; semanal, com retenção de 4 semanas; e mensal, com retenção de 6 meses;

a3) proveniente de banco de dados: diário, com retenção de 28 dias; semanal, com retenção de 12 semanas; e mensal, com retenção de 24 meses.

b) em ambiente de homologação:

b2) proveniente de servidor de aplicação: diário, com retenção de 7 dias; semanal, com retenção de 4 semanas;

b3) proveniente de banco de dados: diário, com retenção de 14 dias; semanal, com retenção de 8 semanas.

IV - quanto à aplicação e retenção do backup realizado em fita:

a) em ambientes de produção e homologação:

a1) diário com retenção de 14 dias, semanal com retenção de 2 semanas, mensal com retenção de 6 meses e anual com retenção de 1 ano.

V - quanto à retenção dos backups realizados na nuvem:

a) Os backups realizados na nuvem terão a mesma retenção dos backups realizados em disco.

VI - quanto à replicação:

a) devem ser feitas cópias dos backups e armazenadas, preferencialmente, em ambientes separados.

VII) quanto aos serviços em nuvem (SaaS):

a) salvaguarda dos dados em formato digital pertencentes a serviços de TIC do Tribunal Regional Eleitoral do Maranhão mas custodiados e/ou controlados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Parágrafo único. Os backups de dados provenientes de fontes não especificadas neste artigo deverão seguir a mesma política especificada para o backup dos servidores de aplicação. Caso não haja distinção entre ambiente de produção e homologação para este ativo, deve ser seguida a política para backup de servidores de aplicação em ambiente de homologação.

Art. 10 Expirado o prazo de retenção dos dados armazenados, o espaço de armazenamento poderá ser reutilizado.

Art. 11 A recuperação de backups deverá obedecer às seguintes orientações:

I - o usuário que necessitar recuperar arquivos deverá registrar o pedido através de chamado contendo, obrigatoriamente, as informações sobre o usuário, o arquivo a ser recuperado, o subdiretório de localização e a data da versão que deseja recuperar;

II - o chamado será encaminhado ao administrador de backup, que após a conclusão da tarefa, realizará o fechamento do chamado indicando ao solicitante a restauração do arquivo;

III - os bancos de dados serão restaurados pelo administrador de recurso, devendo o administrador de backup auxiliá-lo na tarefa de restore.

Art. 12 Os backups de produção deverão ser testados trimestralmente.

§1º Havendo detecção de falha ao efetuar o backup ou se este estiver incompleto, novo backup deverá ser executado com vistas ao seu armazenamento.

§2º Havendo reincidência da execução descrita no §1º deste artigo, o administrador de backup deverá registrar incidente e submetê-lo à apreciação do administrador de recurso com vista à correção da aplicação do backup.

Art. 13 Quaisquer procedimentos programados nos equipamentos computacionais físicos ou virtuais e que impliquem em riscos de funcionamento com interrupção dos sistemas e serviços essenciais do TRE-MA somente deverão ser executados após a realização do backup dos seus dados.

Parágrafo único. Em casos excepcionais em que a urgência justifique, desde que autorizados pelo Secretário de Tecnologia da Informação e Comunicação, os procedimentos mencionados no caput deste artigo poderão ser executados sem a realização de backup.

Art. 14 Fica estabelecido o prazo de sessenta dias, a contar da data de publicação desta Portaria para adoção das providências necessárias à implementação plena desta política de backup.

Art. 15 Revoga-se a Portaria TRE-MA/PR/DG/STIC/CGTIC nº 786/2021.

Art. 16 Esta Portaria entra em vigor na data de sua publicação.

Mário Lobão Carvalho

Diretor-Geral

## DOCUMENTOS ELETRÔNICOS PUBLICADOS PELO PJE

### EDITAIS

#### PRESTAÇÃO DE CONTAS ANUAL(12377) Nº 0600226-65.2023.6.10.0000

PROCESSO : 0600226-65.2023.6.10.0000 PRESTAÇÃO DE CONTAS ANUAL (São Luís - MA)

**RELATOR** : Gabinete Vice-Presidência

FISCAL DA LEI : PROCURADORIA REGIONAL ELEITORAL

INTERESSADO : JOAO CARLOS SOUSA SANTOS NETO

INTERESSADO : JOSE SIMPLICIO ALVES DE ARAUJO

INTERESSADO : LUIZ AMORIM FERNANDES JUNIOR

INTERESSADO : LUIZ RODOLFO BARATA RODRIGUES

INTERESSADO : SAULO GIOVANI MENDONCA

INTERESSADO : WOLMER DE AZEVEDO ARAUJO

REQUERENTE : DIRETÓRIO ESTADUAL DO PARTIDO SOLIDARIEDADE -SD

PODER JUDICIÁRIO

TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO