TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Portaria Presidência Nº 237/2025 TRE/PRESI/DG/ASSDG, de 08 de maio de 2025

Dispõe sobre as regras e os procedimentos para gerenciamento de *backup* e restauração de dados no âmbito da rede corporativa de dados do Tribunal Regional Eleitoral do Piauí (TRE-PI).

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais,

Considerando que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos;

Considerando, ainda, que o acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e da segurança da informação;

Considerando a Resolução CNJ n.º 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

Considerando a Resolução TSE n.º 23.644/2021, que instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

Considerando a Resolução TRE-PI nº 448/2022 que adota a PSI da Justiça Eleitoral estabelecida pela Resolução TSE nº 23.644/2021;

Considerando as boas práticas de segurança da informação previstas nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002;

Considerando as boas práticas de segurança da informação previstas no modelo CIS Controls V.8.

**RESOLVE:**

Art. 1º Fica instituída a norma complementar referente à política de gerenciamento de *backup* e restauração de dados âmbito do Tribunal Regional Eleitoral do Piauí.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021 e Resolução TRE-PI nº 448/2022.

Art. 3º As informações do Tribunal Regional Eleitoral do Piauí, incluindo dados pessoais, biográficos, biométricos e corporativos, devem ser protegidas por

meio de rotinas sistemáticas de *backup*.

Art. 4º Não estão cobertos por esta norma os dados armazenados localmente em microcomputadores, notebooks, dispositivos móveis ou outros dispositivos de uso individual.

Art. 5º A salvaguarda e a recuperação dos dados de sistemas de informação custodiados por outras entidades, públicas ou privadas, utilizados pelo TRE-PI, deverão estar estabelecidas em termos de convênio e/ou cláusulas contratuais respectivamente..

## CAPÍTULO I

## DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para efeitos desta norma consideram-se os termos e definições a seguir:

I - ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

II - atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

III - ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;

IV - ativo de TI: o mesmo que ativo de processamento;

V - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

VI - autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VII - *backup* ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

VIII - *backup* completo: modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backup*;

IX - *backup* diferencial: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;

X - *backup* incremental: modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de

qualquer modalidade efetuado;

XI - equipamento de *backup* em disco: dispositivos de armazenamento de cópias de segurança em disco;

XII - estratégia de salvaguarda de dados: grupo de informações para execução de cópias de segurança de dados agendados;

XIII - confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

XIV - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

XV - custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

XVI - descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;

XVII - gestor de ativo de informação: proprietário ou custodiante de ativo de informação.

XVIII - incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XIX - incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

XX - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

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

XXII - janela de *backup*: período de tempo durante o qual, cópias de segurança sob execução agendada ou manual poderão ser executadas;

XXIII - mídias magnéticas (fitas de *backup*): mídia de armazenamento não-volátil que consiste em uma fita plástica coberta de material magnetizável;

XXIV - local de armazenamento: local onde as cópias de segurança serão armazenadas;

XXV - periodicidade: frequência com que a cópia de segurança é executada;

XXVI - plano de Gerenciamento de *Backup* e Restauração de Dados: Documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da norma complementar da Política de Segurança da Informação para gerenciamento de *backup* e restauração de dados;

XXVII - proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o

qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XXVIII - recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXIX - recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

XXX - rede de computadores: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

XXXI - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de *backup*;

XXXII - retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XXXIII - risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XXXIV - RPO (*recovery point objective*): tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após a ocorrência de um desastre;

XXXV - RTO (*recovery time objective*) ou tempo esperado para restauração: tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre;

XXXVI - rotina de *backup*: procedimento utilizado para se realizar um *backup*;

XXXVII - usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXXVIII - unidade de armazenamento de *backup*: dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

XXXIX - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## CAPÍTULO II

## DOS PADRÕES OPERACIONAIS

### SEÇÃO I

### DOS PRINCÍPIOS GERAIS

Art. 7º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

Art. 8º As rotinas de *backup* devem possuir requisitos mínimos, diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

Art. 9º As tecnologias utilizadas para a realização do *backup* devem cumprir os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações.

Art. 10. Os dados abarcados por esta norma deverão ser definidos em um Plano de Gerenciamento de *Backup* e Restauração de Dados, a ser definido pela área técnica responsável, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos.

Parágrafo único. O Plano de Gerenciamento de *Backup* e Restauração de Dados deve ser aprovado pela Comissão de Segurança da Informação.

Art. 11. O Plano de Gerenciamento de *Backup* e Restauração de Dados deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados a serem salvaguardados/restaurados);

II - tipo (completo/total, incremental e diferencial);

III - frequência (diária, semanal, mensal e anual);

IV - tempo de retenção;

V - unidade de armazenamento;

VI - janela de *backup*;

VII - local de armazenamento das mídias; e

VIII - periodicidade de teste de restauração do *backup*.

Art. 12. A documentação do Plano de Gerenciamento de *Backup* e Restauração de Dados e das rotinas de *backup* deve ser armazenada em local seguro e com acesso restrito à seção responsável pelo gerenciamento de *backup*.

Art. 13. A infraestrutura de *backup* não pode utilizar os mesmos controladores de domínio do restante da infraestrutura e nem os dos usuários comuns, devendo ainda, ficar em rede totalmente apartada e protegida por *firewall*.

Art. 14. Os *backups* devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

Art. 15. Os *backups* devem ser armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Parágrafo único. Deverão ser implementados controles criptográficos nos arquivos que trafegam na rede da organização ou na Internet (*data in transit*).

Art. 16. Deverão ser utilizadas soluções de *backup* e restauração de dados adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

## SEÇÃO II

## DAS ROTINAS TÉCNICAS

Art. 17. A solicitação e validação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada pelos responsáveis técnicos dos serviços de TI.

§1º A conclusão bem sucedida das cópias de segurança deverá ser confirmada, analisando-se, se for o caso, os arquivos de *log*, para verificar o resultado da operação;

§2º Em caso de problemas na operação das cópias de segurança, as causas deverão ser analisadas, reparadas e, quando necessário, uma nova cópia será realizada.

Art. 18. Não serão realizados *backups* referentes à:

I - de computadores servidores de teste e de homologação;

II - de computadores servidores que não estiverem localizados no *Data Center* do TRE-PI;

III - de arquivos armazenados em estações de trabalho;

§ 1º Os *backups* referentes aos equipamentos acima são de responsabilidade única e exclusiva do usuário, que contará com orientações fornecidas pela STI para executar a cópia de segurança e recuperação desses dados.

§ 2º Excepcionalmente, poderá ser realizado *backup* dos servidores de testes e de homologação, com retenção máxima a ser definida pelo requisitante, mediante solicitação expressa dessa necessidade pelo gestor da área demandante e com autorização da STI.

Art. 19. Todas as informações de interesse da instituição deverão ser armazenadas em repositório centralizado que passará por procedimento de *backup* como forma de garantir a integridade, disponibilidade e cópia de segurança da informação, tais como:

I - artefatos e códigos-fonte dos sistemas mantidos pelo TRE-PI;

II - banco de dados;

III - servidores de aplicação;

IV - repositório do sistema de arquivos;

V - configurações de sistemas e logs;

VI - arquivos de auditoria; e

VII - imagens do circuito fechado de câmera de segurança.

Art. 20. Os computadores servidores de produção que armazenem arquivos do tipo texto, documentos e mídia terão sua estratégia de salvaguarda de dados criada sem a necessidade de solicitação.

Art. 21. A cópia de segurança dos bancos de dados deverá ser realizada, pelo menos, quatro vezes ao dia, na modalidade incremental, para reduzir a perda de transações.

Art. 22. A cópia de segurança dos sistemas eleitorais e de seus arquivos de banco de dados será realizada conforme orientações do Tribunal Superior Eleitoral –TSE.

Art. 23. A cópia de segurança dos dados dos servidores de aplicação será realizada de acordo com as especificações definidas pela área responsável pela infraestrutura de serviços de Tecnologia da Informação, com base nas informações prestadas pelo gestor do ativo de informação.

Art. 24. Para servidores virtualizados, será mantida uma cópia mensal em fita e outra em disco, sempre que possível.

## SEÇÃO III

## DOS TIPOS, FREQUÊNCIA E RETENÇÃO DOS DADOS DE BACKUPS

Art. 25. Os *backups* deverão ser realizados observando-se o tipo, a frequência e o tempo de retenção a serem definidos no Plano de Gerenciamento de *Backup* e Restauração de Dados.

§1º Poderão ser estabelecidos tipo, frequência e tempo de retenção diferenciados para cada serviço e/ou sistema de informação, de acordo com o nível de criticidade, desde que respeitados os padrões mínimos estabelecidos no Plano de Gerenciamento de *Backup* e Restauração de Dados.

§2º Os *backups* dos sistemas devem ser realizados utilizando-se os seguintes tipos:

I - completo/total;

II - incremental; ou

III - diferencial.

§3º Os *backups* dos sistemas devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; ou

IV - anual;

Art. 26. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

## SEÇÃO IV

## DO USO DA REDE

Art. 27. Deverá ser considerado, para a execução das rotinas de *backup*, o seu impacto sobre o desempenho da rede computacional, garantindo que o tráfego necessário para tal não cause a indisponibilidade dos demais sistemas e serviços de TI.

Parágrafo único - O *backup* das informações armazenadas nos servidores da rede corporativa deve ser realizado em período de baixa utilização de seus recursos computacionais, preferencialmente fora do horário de expediente ordinário das unidades da Secretaria do Tribunal.

## SEÇÃO V

## DAS UNIDADES DE ARMAZENAMENTO DE BACKUPS

Art. 28. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá atender as seguintes características dos dados resguardados:

I - a criticidade;

II - o tempo de retenção;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração (RTO);

V - o custo de aquisição da unidade de armazenamento de *backup*; e

VI - a vida útil da unidade de armazenamento de *backup*;

Art. 29. O *backup*, de acordo com sua criticidade, deve ser provido em 2 (duas) mídias distintas, com conteúdo idêntico, para armazenamento em 2 (dois) locais diferentes, observado o seguinte:

I - uma cópia de segurança deve ser armazenada de forma a permitir sua rápida localização e recuperação;

II - outra cópia de segurança deve ser armazenada em local externo ao prédio onde é realizado o *backup*;

III - ao menos uma cópia de segurança deve ser armazenada em uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

§1º Os locais de armazenamento das mídias da cópia de segurança devem ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I - o acesso ao local deve ser restrito e monitorado;

II - o acesso ao local deve ser registrado em logs contendo minimamente a identificação do usuário e informações de data e hora de entrada e saída;

III - o local deve possuir controles de prevenção, detecção e combate a incêndio;

IV - o local deve ser protegido contra interferências eletromagnéticas.

§2º Os locais externos de armazenamento da cópia de segurança devem possuir requisitos de segurança adequados e separados do ambiente de armazenagem da cópia principal, de forma que não permaneçam expostos aos mesmos riscos de desastres que a localidade de origem dos dados.

§3º A cópia de segurança referida no inciso II do *caput* pode ser armazenada em serviços de nuvem, desde que sejam criptografados e gerenciados pela mesma solução de *backup*, sendo observados, ainda, os cuidados de gerenciamento de acessos privilegiados e de bloqueio de redes de acesso.

Art. 30. Deverá ser identificada a viabilidade de utilização de diferentes tecnologias na realização dos *backups*, propondo a melhor solução para cada caso.

Art. 31. Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável.

## SEÇÃO VI

## DO DESCARTE E DA SUBSTITUIÇÃO DA CÓPIA DE SEGURANÇA

Art. 32. O descarte e a substituição da mídia utilizada para geração da cópia de segurança devem respeitar o disposto na norma complementar específica da Política de Segurança da Informação que trata do Controle de Acesso Físico e Lógico relativos à Segurança da Informação.

Art. 33. Nos casos de substituição da solução de *backup* (*hardware* ou *software*), as informações contidas nas mídias da antiga solução devem, preferencialmente, ser transferidas, em sua totalidade, para mídias compatíveis com a nova solução.

§1º A solução de *backup* obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.

§2º Havendo possibilidade de manter a solução original até o cumprimento do tempo de retenção das informações em mídias antigas, a transferência não é necessária.

Art. 34. Quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

## SEÇÃO VII

## DOS TESTES DE BACKUP

Art. 35. Os *backups* devem ser testados periodicamente, ao menos mensalmente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Parágrafo único. Caso ocorra falha na restauração, a unidade responsável deverá tomar as medidas necessárias à correção do problema.

Art. 36. Os testes de restauração dos *backups* devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 37. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* devem ser devidamente registradas no Plano de Gerenciamento de *Backup* e Restauração de Dados.

# CAPÍTULO III

# DA RECUPERAÇÃO DE DADOS

Art. 38. A recuperação de dados será realizada mediante solicitação feita à Central de Serviços e com autorização do Secretário de Tecnologia da Informação,

devendo conter, no mínimo, os seguintes requisitos:

I - o nome do computador servidor a ser restaurado, na hipótese de ser uma cópia de segurança de computador servidor;

II - o nome do banco de dados a ser restaurado, na hipótese de ser uma cópia de segurança de arquivos de banco de dados.

III - nos demais casos, a recuperação de dados será realizada mediante solicitação feita à Central de Serviços, devendo conter, no mínimo, as seguintes informações:

a) o nome do arquivo, pasta ou ativo de rede;

b) o nome do computador servidor em que o arquivo ou a pasta estavam armazenados;

c) o caminho de rede onde o arquivo ou a pasta estavam armazenados.

Art. 39. Em todos os casos será informada a data estimada da qual se deseja restaurar o *backup*, devendo os prazos para restauração da cópia de segurança ser incluídos no catálogo de serviços de Tecnologia da Informação.

## CAPÍTULO IV

## DAS RESPONSABILIDADES

Art. 40. A Secretaria de Tecnologia da Informação - STI será responsável pela execução e gestão das rotinas de *backups* e restauração, devendo:

I - planejar os recursos necessários para implantar os requisitos desta norma e do Plano de Gerenciamento de *Backup* e Restauração de Dados;

II - elaborar o Plano de Gerenciamento de *Backup* e Restauração de Dados específico;

III - propor soluções de *backup* das informações produzidas ou custodiadas pelo Tribunal;

IV - providenciar a criação e manutenção dos *backups*;

V - configurar as soluções de *backup*;

VI - realizar manutenções periódicas dos equipamentos utilizados na salvaguarda de dados;

VII - manter as unidades de armazenamento de *backups* funcionais, preservadas e seguras;

VIII - preservar as mídias magnéticas de forma adequada;

IX - verificar periodicamente os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;

X - gerenciar mensagens e registros de auditoria (logs) dos *backups*;

XI - tomar medidas preventivas para evitar falhas;

XII - reportar imediatamente os incidentes ou erros que causem indisponibilidade ou que impossibilitem a restauração dos *backups*;

XIII - providenciar a execução dos testes de restauração;

XIV - restaurar ou recuperar os *backups* em caso de necessidade.

XV - comunicar ao gestor de ativo de informação os erros e ocorrências nos *backups* dos ativos de informação sob sua responsabilidade.

## CAPÍTULO V

## DAS DISPOSIÇÕES FINAIS

Art. 41. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 42. A norma deverá estar totalmente implantada no prazo de 24 (vinte e quatro) meses a contar da publicação.

Art. 43. Esta Norma Complementar deverá ser revisada que se fizer necessário, não excedendo o prazo de 36 meses.

Art. 44. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

Art. 45. Fica revogada a Portaria Presidência nº 423/2018, de 23 de abril de 2018.

**Desembargador SEBASTIÃO RIBEIRO MARTINS**

**Presidente do TRE-PI**

Documento assinado eletronicamente por **Sebastião Ribeiro Martins**, **Presidente**, em 08/05/2025, às 20:23, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0002406411** e o código CRC **D471727D**.


2024
PRÊMIO
CNJ DE
QUALIDADE
Ouro