TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
GABINETE DA PRESIDÊNCIA

PORTARIA Nº 234/2023 - GP

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 Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

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

CONSIDERANDO a Resolução TRE-RN nº 110/2023, que institui a Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

CONSIDERANDO a Portaria DG/TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Norte, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º O gerenciamento de backup e restauração de dados, no âmbito do Tribunal, observará as disposições contidas nesta portaria.

Art. 2º O gerenciamento de backup e restauração de dados objetiva instituir diretrizes, responsabilidades e competências que visam garantir a segurança, integridade e disponibilidade dos dados custodiados pelo Tribunal Regional Eleitoral do Rio Grande do Norte.

Art. 3º As informações do Tribunal Regional Eleitoral do Rio Grande do Norte, 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-RN, deverão estar estabelecidas em cláusulas contratuais.

CAPÍTULO II
DAS DEFINIÇÕES

Art 6º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG/TSE nº 444/2021, além dos seguintes:

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

II - 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;

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

IV - backup incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado;

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

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

VII - plano de gerenciamento de backup e restauração de dados: Documento formal no qual 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;

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

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

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

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

XII - 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.

CAPÍTULO III
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 pelo Comitê de Governança de Tecnologia da Informação e Comunicação – CgovTIC.

Art. 11. A solicitação e validação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada pelos responsáveis técnicos dos serviços de TI.

Art. 12 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. 13. 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;

VIII - periodicidade de teste de restauração do backup;

Art. 14. 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. 15. Os backups devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

Art. 16. 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. 17. Deverão ser utilizadas soluções de backup e restauração de dados adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

Seção II
Dos tipos, frequência e retenção dos dados de backups

Art. 18. Os backups devem 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. 19. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

Seção III
Do uso da rede

Art. 20. 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 IV
Das unidades de armazenamento de backups

Art. 21. 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;

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

VI - a vida útil da unidade de armazenamento de backup.

Art. 22. 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 à sede do Tribunal;

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

Art. 24. Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável.

Seção V
Do descarte e da substituição da cópia de segurança

Art. 25. 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 das Informações.

Art. 26. Nos casos de substituição da solução de backup (hardware ou software), as informações contidas nas mídias da antiga solução devem ser transferidas, em sua totalidade, para mídias compatíveis com a nova solução.

Art. 27. 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.
Parágrafo único. A solução de backup obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.

Seção VI
Dos testes de backup

Art. 28. Os backups devem ser testados periodicamente, ao menos mensalmente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 29. 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. 30. 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 IV
DAS RESPONSABILIDADES

Art. 31. São atribuições dos responsáveis pela execução e gestão das rotinas de backup e restauração:

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

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

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

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

IX - tomar medidas preventivas para evitar falhas;

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

XI - providenciar a execução dos testes de restauração; E

XII - restaurar ou recuperar os backups em caso de necessidade.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 32. Esta portaria deverá ser revisada a cada 12 meses.

Art. 33. Os casos omissos e eventuais dúvidas quanto à aplicação desta norma serão dirimidos pela Comissão Permanente de Segurança da Informação deste Tribunal.

Art. 34. Revogam-se as disposições em contrário, em especial, a Portaria GP n.º 130, de 24 de abril de 2017.

Art. 35. Esta Portaria entra em vigor na data de sua publicação e sua implementação iniciará imediatamente e deverá estar totalmente implantada no prazo de 24 (vinte e quatro) meses a contar desta data.

Natal/RN, 12 de dezembro de 2023.

Desembargador **Cornélio Alves**
Presidente