PORTARIA PRE Nº 219, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC6 — Geração e Restauração de Cópias de Segurança (Backup) do Tribunal Regional Eleitoral de Minas Gerais.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições conferidas pelo inciso XV do art. 22 da Resolução TRE-MG nº 1.277, de 29 de maio de 2024, o Regimento Interno, considerando o disposto no art. 4° da Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023, que determina que a revisão e a atualização das normas complementares de Segurança da Informação ocorrerão sempre que necessário, por meio de portaria da Presidência do Tribunal,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a Norma de Segurança Cibernética — NSC6 — Geração e Restauração de Cópias de Segurança (*Backup*) do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece as regras gerais para o gerenciamento de *backup* e restauração de dados e institui diretrizes.

Art. 2° Esta portaria integra a Política de Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais, regulamentada pela Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023.

Art. 3° Para os efeitos desta portaria, aplicam-se os termos e definições da Norma de Segurança Cibernética — NSC1 — Termos e Siglas de Segurança da Informação.

Art. 4° Esta portaria aplica-se aos magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizam os ativos de informação e de processamento na Justiça Eleitoral de Minas Gerais.

CAPÍTULO II

DOS PRINCÍPIOS GERAIS

Art. 5° As informações do Tribunal Regional Eleitoral Minas Gerais, incluindo dados pessoais, biográficos, biométricos e corporativos, serão protegidas por meio de rotinas sistemáticas de *backup*.

Art. 6° Esta portaria não abrange os dados armazenados localmente em microcomputadores, *notebooks*, dispositivos móveis ou outros dispositivos de uso individual.

Art. 7° A salvaguarda e a recuperação dos dados de sistemas de informação custodiados por outras entidades, públicas ou privadas, utilizados pelo Tribunal, estarão estabelecidas em cláusulas contratuais.

Art. 8° 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 Tecnologia da Informação e Comunicação — TIC.

Art. 9º As rotinas de *backup* possuirão requisitos diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da organização.

Art. 10. As tecnologias utilizadas para a realização do *backup* cumprirão os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações.

Art. 11. Os dados abarcados por esta portaria serão 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 será aprovado pela Comissão de Segurança da Informação — CSI.

Art. 12. A solicitação e a validação de salvaguarda dos dados referentes aos serviços de TIC serão realizadas pelos seus responsáveis técnicos.

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

Art. 14. O Plano de Gerenciamento de *Backup* e Restauração de Dados explicitará os seguintes requisitos técnicos:

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

II — tipo (completo/total, incremental ou 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. 15. A documentação do Plano de Gerenciamento de *Backup* e Restauração de Dados e das rotinas de *backup* será armazenada em local seguro e com acesso restrito à seção responsável pelo gerenciamento de *backup*.

Art. 16. Os *backups* estarão em conformidade com a legislação vigente, em especial ao que compete à Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais — LGPD.

Art. 17. Os *backups* serão armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

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

Art. 18. Serão utilizadas soluções de *backup* e restauração de dados adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

Art. 19. A solicitação para restauração de *backup* será definida e autorizada através de procedimento a ser previsto na Política de *Backup.*

CAPÍTULO III

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

Art. 20. Os *backups* serão realizados observando-se o tipo, a frequência e o tempo de retenção.

Art. 21. Para cada serviço e/ou sistema de informação, poderão ser estabelecidos tipo, frequência e tempo de retenção diferenciados, de acordo com o nível de criticidade, podendo ser estabelecidos novos padrões no Plano de Gerenciamento de *Backup* e Restauração de Dados, desde que observados os padrões necessários.

Art. 22. Os *backups* dos sistemas serão realizados utilizando-se os seguintes tipos:

I — completo/total;

II — incremental;

III — diferencial.

Art. 23. Os *backups* dos sistemas serão realizados utilizando-se as seguintes frequências temporais:

I — diária;

II — semanal;

III — mensal;

IV — anual.

Art. 24. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

CAPÍTULO IV

DO USO DA REDE

Art. 25. Será 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 TIC.

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

CAPÍTULO V

DAS UNIDADES DE ARMAZENAMENTO DE *BACKUPS*

Art. 26. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados atenderá 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*;

VI — a vida útil da unidade de armazenamento de *backup*.

Art. 27. O *backup*, de acordo com sua criticidade, será provido em 2 (duas) mídias distintas, com conteúdo idêntico, para armazenamento em 2 (dois) locais diferentes, observado o seguinte:

I — 1 (uma) cópia de segurança será armazenada de forma a permitir sua rápida localização e recuperação;

II — 1 (uma) cópia de segurança será armazenada em local externo à sede do Tribunal;

III — ao menos 1 (uma) cópia de segurança será armazenada em uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

Art. 28. Os locais de armazenamento das mídias da cópia de segurança terão mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I — o acesso ao local será restrito e monitorado;

II — o acesso ao local será registrado em *logs* contendo minimamente a identificação do usuário e informações de data e hora de entrada e saída;

III — o local possuirá controles de prevenção, detecção e combate a incêndio;

IV — o local será protegido contra interferências eletromagnéticas.

Art. 29. Os locais externos de armazenamento da cópia de segurança possuirão 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.

Art. 30. A cópia de segurança poderá 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. 31. Será identificada a viabilidade de utilização de diferentes tecnologias na realização dos *backups*, propondo a melhor solução para cada caso.

Art. 32. Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável.

CAPÍTULO VI

DO DESCARTE E DA SUBSTITUIÇÃO DA CÓPIA DE SEGURANÇA

Art. 33. O descarte das mídias utilizadas para *backup* será realizado em conformidade com as recomendações dos fabricantes e as boas práticas mercadológicas existentes e de forma a impossibilitar a recuperação total ou parcial das informações.

Art. 34. Nos casos de substituição da solução de *backup* (*hardware* ou *software*), as informações contidas nas mídias da antiga solução serão transferidas, em sua totalidade, para mídias compatíveis com a nova solução.

Art. 35. Quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos serão 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.

CAPÍTULO VII

DOS TESTES DE *BACKUP*

Art. 36. Os *backups* serão testados com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 37. Os testes de restauração dos *backups* serão realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 38. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* serão devidamente registrados no Plano de Gerenciamento de *Backup* e Restauração de Dados.

CAPÍTULO VIII

DAS RESPONSABILIDADES

Art. 39. São atribuições dos responsáveis pela execução e gestão das rotinas de *backup* e restauração:

I — planejar os recursos necessários para implantar os requisitos desta portaria 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 — 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;

XII — restaurar ou recuperar os *backups* em caso de necessidade.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 40. Esta portaria trata de temas gerais, devendo ser observada a política de *backup* instituída pela Portaria n° 38, de 14 de maio de 2018, da Presidência.

Art. 41. O descumprimento desta portaria será imediatamente registrado como incidente de segurança e comunicado à Comissão de Segurança da Informação para apuração e consequente adoção das providências cabíveis.

Art. 42. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 43. Esta portaria entra em vigor na data de sua publicação.

Belo Horizonte, 16 de setembro de 2024.

Desembargador Ramom Tácio de Oliveira
Presidente

Documento assinado eletronicamente por **RAMOM TÁCIO DE OLIVEIRA**, **Presidente**, em 16/09/2024, às 16:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **5680253** e o código CRC **86A8DB7E**.