



TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS
AV. PRUDENTE DE MORAIS, 100 - Bairro CIDADE JARDIM - CEP 30380000 - Belo Horizonte - MG

PORTARIA PRE Nº 220, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética – NSC7 –
Continuidade de Serviços Essenciais de TIC 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. 4º 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.”;

CONSIDERANDO o disposto na Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação da Justiça Eleitoral – PSI-JE;

CONSIDERANDO o disposto na Resolução TRE-MG nº 1.190, de 21 de setembro de 2021, que institui a Política de Continuidade dos Serviços Essenciais de Tecnologia da Informação e Comunicação do Tribunal;

CONSIDERANDO o disposto na Resolução TRE-MG nº 1.268, de 30 de janeiro de 2024, que dispõe sobre a Gestão de Crise e de Continuidade de Negócios e sobre o Plano de Continuidade de Negócios bem como institui o Comitê de Gestão de Crise e de Continuidade de Negócios no Tribunal Regional Eleitoral de Minas Gerais,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Norma de Segurança Cibernética – NSC7 – Continuidade de Serviços Essenciais de TIC do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata *o caput* estabelece as principais estratégias para garantir a continuidade de serviços essenciais de Tecnologia da Informação e Comunicação do Tribunal Regional Eleitoral de Minas Gerais em caso de desastre.

Art. 2º 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. 3º 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. 4º 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

DO PLANO DE CONTINUIDADE DOS SERVIÇOS ESSENCIAIS DE TIC

Art. 5º Será elaborado um Plano de Continuidade dos Serviços Essenciais de TIC – PCTIC –, considerando os processos e ativos críticos, no prazo máximo de 180 (cento e oitenta) dias, contados da publicação desta portaria.

Art. 6º A Secretaria de Tecnologia da Informação – STI – elaborará o PCTIC em conjunto com as áreas técnicas, conforme níveis de serviço previstos no capítulo III e em consonância com a Gestão de Continuidade de Negócios, estabelecida pela Resolução TRE-MG nº 1.268, de 30 de janeiro de 2024.

Art. 7º Para a elaboração do PCTIC, serão analisados e observados:

I – o Plano de Continuidade de Negócios – PCN–, que será elaborado pelo Comitê Gestor de Continuidade de Negócios – CGCN;

II – os sistemas e aplicativos descritos como essenciais ou críticos para o negócio, conforme definidos em publicação específica;

III – os macroprocessos de trabalho e sua importância para a organização;

IV – a infraestrutura tecnológica em uso ou em implantação.

Art. 8º O PCTIC será apresentado à Comissão de Segurança da Informação – CSI – e ao CGCN para validação.

Art. 9º O PCTIC será aprovado pelo Comitê Executivo de TIC – CETIC – e publicado somente na *intranet*, com acesso restrito, evitando exposição desnecessária de informações relativas à segurança do ambiente computacional.

Art. 10. O CETIC é o responsável por elaborar e manter a documentação sobre o PCTIC.

Art. 11. O PCTIC será testado semestralmente, na mesma data ou em partes, de acordo com a maturidade e com a disponibilidade das equipes técnicas.

Art. 12. O resultado dos testes será documentado e posteriormente avaliado pelo CETIC, que poderá solicitar ajustes ou outras providências.

Art. 13. O PCTIC terá cópias físicas impressas em locais de fácil acesso aos gestores das equipes técnicas responsáveis pela sua execução.

Art. 14. A política de cópias de segurança (*backup*) suportará os níveis de serviço previstos neste capítulo.

CAPÍTULO III DAS PERDAS E INTERRUPÇÕES

Art. 15. O Tempo de Recuperação Objetivado – TRO/RTO – fica definido em:

I – sistemas críticos: 48 (quarenta e oito) horas;

II – sistemas não-críticos: 72 (setenta e duas) horas;

III – serviços básicos de rede (*Domain Name System – DNS –*, *Dynamic Host Configuration Protocol – DHCP –* e autenticação *Active Directory – AD*): 24 (vinte e quatro) horas;

IV – sistemas de homologação e testes: sem tempo definido.

Art. 16. O Ponto de Recuperação Objetivado – PRO/RPO – fica definido em:

I – sistemas críticos: 24 (vinte e quatro) horas;

II – sistemas não-críticos: 72 (setenta e duas) horas;

III – infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (*Active Directory* e *Single-Sign-On*): 6 (seis) horas.

Art. 17. O Período Máximo de Interrupção Tolerável – PMIT/MTO – fica definido em:

I – sistemas críticos: 72 (setenta e duas) horas;

II – sistemas não-críticos: 168 (cento e sessenta e oito) horas;

III – infraestrutura de rede, incluindo equipamentos de comunicação, infraestrutura de virtualização, servidores de DNS e DHCP, serviços de autenticação (*Active Directory* e *Single-Sign-On*): 48 (quarenta e oito) horas;

IV – sistemas de homologação e testes: sem tempo definido.

CAPÍTULO IV DAS DISPOSIÇÕES FINAIS

Art. 18. 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. 19. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 20. 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 **5680265** e o código CRC **3061D2D4**.

0022358-43.2023.6.13.8000

5680265v1