PORTARIA PRE Nº 226, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC13 — Gestão de Vulnerabilidades, em consonância com a Política de Segurança da Informação — PSI — 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 — NSC13 — Gestão de Vulnerabilidades, em consonância com a Política de Segurança da Informação — PSI — do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece as principais estratégias para gestão de vulnerabilidades para os ativos de Tecnologia da Informação e Comunicação — TIC — do Tribunal Regional Eleitoral de Minas Gerais.

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.

Art. 5° A gestão de vulnerabilidades tem como objetivo prevenir a exploração de vulnerabilidades técnicas na rede corporativa, por meio da aplicação sistemática das seguintes ações de prevenção, identificação, classificação e tratamento:

I — criptografia dos dados sigilosos e sensíveis;

II — identificação de vulnerabilidades técnicas em tempo hábil;

III — avaliação de exposição às vulnerabilidades técnicas;

IV — adoção de medidas apropriadas e tempestivas para lidar com os riscos identificados.

CAPÍTULO II

DO MONITORAMENTO DE BASES DE VULNERABILIDADES

Art. 6° Os controles estabelecidos serão aplicados para monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta para obtenção de informações relacionadas a vulnerabilidades técnicas e medidas de correção, definindo-se a relação de fontes de consulta de acordo com os critérios abaixo:

I — qualidade das informações — verificar se as informações fornecidas pela fonte são precisas e atualizadas;

II — disponibilidade das informações — verificar a frequência de atualização das informações fornecidas pela fonte;

III — legitimidade da fonte — verificar se a fonte é representante autorizado do responsável pela informação ou reconhecida como confiável pela comunidade de segurança da informação;

IV — obtenção de informações sobre vulnerabilidades técnicas e medidas de correção, incluindo:

a) notícias e alertas sobre ameaças, vulnerabilidades, ataques e *patches*, com especial atenção às "vulnerabilidades de dia zero";

b) melhores práticas de segurança da informação adotadas pelo mercado, políticas, procedimentos, diretrizes e listas de verificação;

c) tendências do mercado de segurança da informação relacionadas ao setor, leis e regulamentos, requisitos de clientes e soluções de fornecedores;

d) dados sobre segurança da informação de consultorias especializadas, outras organizações, polícia, agências de segurança do governo ou congêneres;

e) notícias relacionadas a novas tecnologias e produtos.

CAPÍTULO III

DA DESCOBERTA DE VULNERABILIDADES TÉCNICAS

Art. 7° Os controles estabelecidos serão aplicados para utilizar regularmente ferramentas automatizadas e rotinas para a identificação de vulnerabilidades técnicas na rede corporativa, realizando-se as seguintes atividades:

I — empregar ferramenta atualizada de varredura de vulnerabilidades para investigar automaticamente os ativos e identificar vulnerabilidades na rede corporativa, considerando pelo menos as seguintes características:

a) utilização da fonte *Common Vulnerabilities and Exposures* — CVE — como base para a verificação de vulnerabilidades nos ativos de processamento;

b) compatibilidade com *Security Content Automation Protocol* — SCAP — ou

outro protocolo de automatização da verificação de configurações de segurança;

II — assegurar que somente varreduras de vulnerabilidades autorizadas possam ser executadas, local ou remotamente, e configuradas com direitos elevados nos ativos de processamento que estão sendo testados;

III — usar credencial (ou conta de acesso) dedicada para varreduras de vulnerabilidades, que não deve ser usada para outras atividades administrativas.

CAPÍTULO IV

DA AVALIAÇÃO DA EXPOSIÇÃO

Art. 8° Os controles estabelecidos serão aplicados para analisar e avaliar os riscos de as vulnerabilidades técnicas afetarem o ambiente da rede corporativa, executando-se as seguintes tarefas:

I — consulta de inventário de ativos para identificar quais ativos de processamento serão afetados pela vulnerabilidade técnica, o valor dos ativos para a organização, os requisitos de segurança da informação e a classificação de segurança;

II — verificação de como a vulnerabilidade técnica pode afetar o ambiente da rede corporativa, considerando interfaces e interdependências internas e externas, requisitos de segurança da informação implementados e classificação de segurança dos ativos de processamento críticos;

III — avaliação quanto à necessidade de criar ambiente de teste, realização de provas de conceito (*Proofs of Concept* ou PoCs), desativação de serviços/funcionalidades ou aplicação de *patches* de correção;

IV — documentação de procedimentos para correção da vulnerabilidade técnica, contemplando instalação, configuração, regras estabelecidas e procedimentos de restauração;

V — utilização de classificação de risco para priorizar a correção da vulnerabilidade técnica, conforme nível de criticidade, potencial de dano, facilidade de exploração da ameaça e nível de sigilo das informações acessadas pelo ativo;

VI — comunicação imediata à Comissão de Segurança da Informação sobre a impossibilidade de tratamento de vulnerabilidade técnica classificada como crítica;

VII — geração de registro do incidente.

CAPÍTULO V

DO TRATAMENTO DE VULNERABILIDADES TÉCNICAS

Art. 9º Os controles estabelecidos serão aplicados para corrigir as vulnerabilidades técnicas ou minimizar a probabilidade de exploração, executando-se as seguintes tarefas:

I — observância da norma vigente de Tratamento e Resposta a Incidentes em Redes de Computadores;

II — adoção de testes e homologação da correção da vulnerabilidade técnica antes de ser instalada no ambiente da rede corporativa;

III — atualização dos procedimentos para correção da vulnerabilidade técnica, contemplando instalação, configuração, regras estabelecidas e procedimentos de restauração, quando for o caso;

IV — geração de registros de eventos (*logs*) das ações realizadas para correção da vulnerabilidade técnica, identificados de forma distinta.

Art. 10. Quando não existir a possibilidade de correção da vulnerabilidade - por impossibilidade de atualização de *software* ou de alteração de configuração, desde que devidamente justificado, será considerado o uso dos seguintes controles:

I — desativação de serviços relacionados à vulnerabilidade;

II — aumento do monitoramento relacionado ao ativo para detectar ou prevenir ataques reais;

III — aumento da conscientização sobre a vulnerabilidade;

IV — implementação de controles de segurança compensatórios.

Art. 11. As mudanças no ambiente da rede corporativa motivadas pelas correções das vulnerabilidades técnicas serão implantadas de acordo com o processo vigente de Gerência de Mudanças.

CAPÍTULO VI

DA AVALIAÇÃO DE RESULTADOS

Art. 12. Os controles estabelecidos serão aplicados para analisar criticamente os resultados da gestão de vulnerabilidades, executando-se as seguintes tarefas:

I — comparação regular dos resultados dos tratamentos de vulnerabilidades técnicas consecutivas para verificar se foram corrigidas em tempo hábil;

II — acompanhamento regular do nível de exposição dos principais ativos de processamento;

III — comunicação periódica à Comissão de Segurança da Informação — CSI —, através de relatórios estatísticos, a respeito dos resultados de detecção e tratamento das vulnerabilidades no ambiente computacional;

IV — proposição de melhorias nos processos da gestão de vulnerabilidades para a CSI.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 13. Para assegurar a rastreabilidade adequada das vulnerabilidades técnicas, serão observadas as seguintes responsabilidades e competências na segurança da informação:

I — caberá ao setor responsável pela segurança cibernética:

a) monitorar regularmente sítios de fabricantes, fóruns especializados, grupos especiais e outras fontes de consulta, para obter informações relacionadas a vulnerabilidades técnicas e medidas de correção;

b) acionar ferramentas automatizadas e métodos para a identificação de vulnerabilidades técnicas no ativo, assegurando a execução de verificações na periodicidade mínima definida para cada tipo de ativo, conforme NSC2 – Gestão de Segurança Cibernética em Ativos;

c) analisar e avaliar os riscos das vulnerabilidades técnicas detectadas;

d) comunicar-se com a Equipe de Tratamento e Resposta a incidentes em Redes e Ambientes Computacionais — ETIR — e com as áreas da Secretaria de Tecnologia da Informação — STI — responsáveis pelos ativos, a fim de informar e obter informações acerca de vulnerabilidades existentes;

e) acompanhar a detecção e o tratamento das vulnerabilidades através de ferramenta automatizada específica e documentação produzida pelas unidades;

f) reportar à CSI a análise crítica dos resultados da gestão de vulnerabilidades e proposição de melhorias nos processos;

II — caberá à unidade responsável pela administração do ativo:

a) planejar e corrigir as vulnerabilidades técnicas encontradas ou aplicar controles para minimizar a probabilidade de exploração enquanto não for possível a correção definitiva;

b) documentar vulnerabilidades detectadas e correções aplicadas;

c) documentar justificativa para correções não aplicadas.

Art. 14. Os relatórios e registros gerados no processo de gestão de vulnerabilidades de ativos de Tecnologia de Informação — TI — serão tratados e armazenados de forma segura e com acesso reservado às unidades envolvidas no processo.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 15. 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. 16. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 17. 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 16:41, 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 **5680404** e o código CRC **852480D2**.