PORTARIA PRE Nº 222, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC9 — Configuração Segura 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 — NSC9 — Configuração Segura do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece as principais estratégias para padrões de configuração segura para os ativos de Tecnologia da Informação — TI — do Tribunal Regional 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° Para os efeitos desta portaria, será realizada a classificação de risco dos dados conforme definição da Política de Gestão de Riscos do TRE-MG, disposta pela Resolução

Art. 6° Os controles definidos nesta portaria visam estabelecer e manter a configuração segura de ativos corporativos de acordo com a classificação estabelecida na NSC2 — Gestão de Segurança Cibernética em Ativos do Tribunal Regional Eleitoral de Minas Gerais.

CAPÍTULO II

DA CONFIGURAÇÃO SEGURA

Seção I

Para os Ativos de Infraestrutura de Rede

Art. 7° Será estabelecido e mantido um procedimento de configuração segura para os ativos de rede contemplando:

I — revisão e atualização da documentação anualmente ou quando ocorrerem mudanças significativas no ambiente que possam impactar esta medida de segurança;

II — atualização automatizada da documentação, quando possível.

Art. 8° O gerenciamento dos ativos e *softwares* corporativos com implementações de gestão de configuração contemplará, no mínimo:

I — uso de infraestrutura como código (IaC), qual seja, o gerenciamento e provisionamento da infraestrutura por meio de códigos, em vez de processos manuais;

II — acesso a interfaces administrativas por meio de protocolos de rede seguros;

III — não utilização de protocolos de gestão inseguros, a menos que seja operacionalmente essencial e evidenciada a inviabilidade de uso dos protocolos seguros;

IV — aplicação de procedimentos de *hardening* nos ativos de rede e servidores, contemplando a limitação do acesso à interface de gerência em interfaces e/ou endereços IP controlados;

V — implementação de Múltiplo Fator de Autenticação — MFA — sempre que possível.

Seção II

Para os Ativos de Aplicações

Art. 9º Será estabelecido e mantido um processo de configuração segura para os *softwares* de sistemas operacionais e aplicações utilizados nos ativos corporativos que contemple:

I — revisão e atualização da documentação anualmente ou quando ocorrerem mudanças significativas no Tribunal que possam impactar esta medida de segurança;

II — criação de processos automatizados que definam as configurações de segurança dos sistemas para atender aos requisitos de proteger os dados usados nos ativos corporativos;

III — utilização de configurações de *baseline* de segurança com base nos requisitos de segurança ou classificação dos dados no ativo corporativo contemplando:

a) instalação do *software* básico do sistema operacional e posterior aplicação

dos *patches* de segurança apropriados;

b) instalação apenas dos pacotes, ferramentas e utilitários de *software* de aplicação apropriados e atualizações apropriadas ao *software* instalado;

c) execução de processos automatizados de configuração de segurança;

d) execução de testes para aferição da qualidade das implementações de segurança.

Seção III

Para os Ativos de Usuários

Art. 10. Será estabelecido e mantido um processo de configuração segura para os ativos de usuários da rede corporativa do Tribunal que contemple:

I — a configuração de bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade:

a) para sistemas operacionais de uso geral, o período não deve exceder 15 (quinze) minutos;

b) para dispositivos móveis de usuário final, o período não deve exceder 2 (dois) minutos;

II — a desativação ou inutilização das contas padrão nos ativos e *softwares* corporativos quando possível.

Seção IV

Para os Ativos de Dispositivos

Art. 11. Será estabelecido e mantido um processo de configuração segura para os ativos de dispositivos dos usuários da rede corporativa da Justiça Eleitoral que contemple:

I — a implementação e gerenciamento de *firewall* nos servidores, onde houver suporte — *firewall* virtual, *firewall* do sistema operacional ou um agente de *firewall* de terceiros;

II — a implementação e gerenciamento de *firewall* baseado em *host* ou uma ferramenta de filtragem de porta nos dispositivos de usuário final, com uma regra de negação padrão de bloqueio de todo o tráfego, exceto os serviços e portas que são explicitamente permitidos;

III — a desinstalação ou desativação de todos os serviços desnecessários nos ativos e *softwares* corporativos;

IV — a configuração de servidores *Domain Name System* — DNS — confiáveis nos ativos corporativos, preferencialmente servidores DNS controlados pela Justiça Eleitoral e/ou servidores DNS confiáveis acessíveis externamente, caso seja imprescindível para a operação;

V — a imposição de bloqueio automático do dispositivo seguindo um limite pré-determinado de tentativas de autenticação local com falha nos dispositivos portáteis de usuário final, quando compatível:

a) para *laptops*, não serão permitidas mais de 10 (dez) tentativas de autenticação com falha;

b) para *tablets* e *smartphones*, não serão permitidas mais do que 7 (sete) tentativas de autenticação com falha;

VI — a limpeza remota dos dados corporativos de dispositivos portáteis de usuário final de propriedade do Tribunal para dispositivos perdidos ou roubados, ou quando do

desligamento do usuário das atividades exercidas no Tribunal;

VII — a implementação da segmentação dos espaços de trabalho corporativos que sejam utilizados nos dispositivos móveis de usuário final, onde houver suporte, para garantir a separação das aplicações e dados corporativos das aplicações e dados pessoais.

CAPÍTULO III

DAS DISPOSIÇÕES FINAIS

Art. 12. 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. 13. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 14. 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 **5680277** e o código CRC **C87193A0**.