PORTARIA PRE Nº 225, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC12 — Uso de Recursos Criptográficos 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 — NSC12 — Uso de Recursos Criptográficos do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* estabelece o uso de recursos criptográficos, com o objetivo de proteger a confidencialidade, a integridade e a autenticidade dos dados transmitidos pelas redes de computadores, assim como dos dados em repouso, armazenados em servidores, microcomputadores, dispositivos móveis e bancos de dados.

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

DA CRIPTOGRAFIA DOS DADOS EM TRÂNSITO

Art. 5° É obrigatório o uso de protocolo seguro, como *Hypertext Transfer Protocol Secure* — HTTPS —, em todos os sistemas e portais *web*, independentemente de serem acessados pela rede interna ou pela *internet*.

Art. 6° Toda comunicação cliente/servidor, onde trafeguem dados pessoais ou *logins* e senhas, utilizará protocolos de comunicação segura.

Art. 7° Os dados pessoais sensíveis serão armazenados em servidores e em bancos de dados com uso de técnicas de criptografia ou anonimização, visando diminuir o risco em caso de vazamento de dados.

CAPÍTULO III

DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS

Art. 8° Em cópias de segurança (*backups*) que contenham dados pessoais sensíveis, serão adotadas técnicas de criptografia, visando diminuir o risco em caso de vazamento de dados.

Art. 9º Os computadores, *notebooks* e dispositivos móveis, de propriedade da Justiça Eleitoral, terão seus discos rígidos protegidos por criptografia, visando diminuir o risco de vazamento de dados em caso de furto.

CAPÍTULO IV

DO DESENVOLVIMENTO

Art. 10. Quanto à utilização de criptografia nos sistemas, será observado o seguinte:

I — criptografar dados sigilosos e sensíveis;

II — utilizar método de encriptação com parâmetros públicos e documentados e somente a chave criptográfica deve ser mantida em sigilo;

III — nunca utilizar um cifrador que admita um método conhecido para quebra da chave criptográfica por força bruta, baseada em tentativa e erro;

IV — nunca utilizar um tamanho da chave menor que 128 (cento e vinte e oito) *bits* (cifrador simétrico) ou 1024 (mil e vinte e quatro) *bits* (cifrador assimétrico);

V — nunca utilizar função de *hash* sem algum tipo de *Salt*;

VI — nunca utilizar algoritmos considerados obsoletos para criptografia e *hash* criptográfico;

VII — nunca distribuir chaves criptográficas sem a utilização de uma infraestrutura de chave pública e, portanto, sem a utilização de um cifrador assimétrico.

Art. 11. Quanto ao uso de criptografia, é recomendável:

I — evitar utilizar um tamanho da chave menor que 256 (duzentos e cinquenta e seis) *bits* (cifrador simétrico) ou 4096 (quatro mil e noventa e seis) *bits* (cifrador

assimétrico);

II — evitar utilizar módulos criptográficos com geradores de números pseudoaleatórios de alta aleatoriedade para a geração de todos os números, nomes de arquivos, *GUIDs* e *strings* aleatórias;

III — utilizar *hashes* criptográficos sempre que possível, sobretudo nos casos de verificação da integridade de dados, armazenamento e verificação de senhas e provimento de identificador único para objetos em um sistema e geração de números pseudoaleatórios.

CAPÍTULO V

DA ASSINATURA DIGITAL

Art. 12. A Secretaria de Tecnologia da Informação — STI — distribuirá e gerenciará certificados para assinatura digital, sejam do tipo A1 (arquivo digital com senha) ou A3 (*token*), de acordo com as necessidades do usuário interno e com os procedimentos técnicos adotados.

Art. 13. Os certificados digitais poderão ser utilizados como segundo fator de autenticação (2FA) em computadores ou sistemas, de acordo com a sua criticidade e disponibilidade da tecnologia.

CAPÍTULO VI

DA AUTORIDADE CERTIFICADORA

Art. 14. O Tribunal poderá manter Infraestrutura de Chaves Públicas — ICP — própria para uso em sistemas e computadores de uso interno, sendo permitido o modelo de Autoridade Certificadora — AC — autoassinada.

Art. 15. Os certificados digitais instalados em servidores e sistemas *Web* com acesso pela *internet* utilizarão certificados digitais fornecidos por AC comercial, visando a compatibilidade com os computadores e dispositivos móveis dos usuários externos.

CAPÍTULO VII

DAS RESPONSABILIDADES

Art. 16. Caberá à STI, por meio de suas áreas técnicas:

I — implementar o nível adequado de criptografia nos sistemas e dispositivos;

II — adquirir e gerenciar os certificados digitais para usuários;

III — implementar e manter Infraestrutura de Chaves Públicas interna;

IV — adquirir e gerenciar os certificados digitais para servidores e aplicações;

V — informar à Comissão de Segurança da Informação eventuais não-conformidades.

Art. 17. Caberá ao usuário:

I — zelar pela segurança do certificado digital recebido, não compartilhando o seu uso e a sua senha com terceiros;

II — assinar termo de compromisso no ato do recebimento de certificado digital;

III — informar imediatamente o extravio ou o comprometimento do certificado digital à STI, para adoção das providências de revogação.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 18. No caso de algum equipamento, aplicação, aplicativo, sistema ou banco de dados não permitir a adoção de protocolos seguros, essa informação constará em documento de análise de riscos de segurança da informação, imediatamente submetido à Comissão de Segurança da Informação — CSI.

Art. 19. O descumprimento desta portaria será imediatamente registrado como incidente de segurança da informação e comunicado à Comissão de Segurança da Informação para apuração e consequente adoção das providências cabíveis.

Art. 20. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 21. 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 **5680399** e o código CRC **8A3BB9B3**.