TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO

INSTRUÇÃO NORMATIVA Nº 2, DE 05 JUNHO DE 2024

Dispõe sobre as regras e os procedimentos para o uso de recursos criptográficos do Tribunal Regional Eleitoral do Maranhão.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO, no uso das suas atribuições que lhe são conferidas pelo art. 49 do Regulamento Interno da Secretaria do Tribunal Regional Eleitoral do Maranhão, e

CONSIDERANDO a necessidade de definir processos para o uso de recursos criptográficos;

CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNTISO/IEC 27001 e ABNT NBR ISO/IEC 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Maranhão;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Instrução Normativa para o uso de recursos criptográficos.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Res. TSE 23.644/2021.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se os termos e definições previstos na portaria DG-TSE 444/2021.

Art. 4º O uso de recursos criptográficos visa 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.

CAPÍTULO III
DA CRIPTOGRAFIA DOS DADOS EM TRÂNSITO

Art. 5º É obrigatório o uso de protocolo seguro, como HTTPS, em todos os sistemas e portais web, independentemente de serem acessados pela rede interna ou pela Internet.

Art. 6º Toda comunicação cliente/servidor onde trafegam dados pessoais ou logins e senhas, deve utilizar protocolos de comunicação segura.

CAPÍTULO IV
DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS

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

Art. 8º As cópias de segurança (backups) que contenham dados pessoais sensíveis devem adotar técnicas de criptografia, visando diminuir o risco em caso de vazamento de dados.

Art. 9º Os computadores e notebooks de propriedade da Justiça Eleitoral, utilizados em trabalho remoto, devem ter seus discos rígidos protegidos por criptografia, visando diminuir o risco de vazamento de dados em caso de furto.

CAPÍTULO V
DA ASSINATURA DIGITAL

Art. 10 A STIC deverá distribuir e gerenciar 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. 11 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. 12 O TRE-MA poderá manter infraestrutura de Chaves Públicas (ICP) própria para uso em sistemas e computadores de uso interno, sendo permitido o modelo de AC (autoridade certificadora) auto assinada.

Art. 13 Os certificados digitais instalados em servidores e sistemas Web com acesso pela Internet deverão utilizar certificados digitais fornecidos por AC (autoridade certificadora) comercial, visando a compatibilidade com os computadores e dispositivos móveis dos usuários externos.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 14 – Cabe à STIC, 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 ao Comitê Gestor de Segurança da Informação eventuais não-conformidades.

Art. 15 – Cabe ao usuário:

I – Zelar pela sua 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 à STIC em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação.

IV - O usuário deve estar ciente de que a assinatura ou login feitos por meio de certificado digital são irretratáveis, não podendo este alegar que não efetuou a ação, exceto em caso de fraude ou falha comprovada da autoridade certificadora.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 16 No caso de algum equipamento, aplicação, aplicativo, sistema ou banco de dados não permitir a adoção de protocolos seguros, a informação deverá constar em documento de análise de riscos de segurança da informação, sendo imediatamente submetido para apreciação do Comitê Gestor de Segurança da Informação.

Art. 17 Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação.

Art. 18 A STIC elaborará, em até 120 dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.

Art. 19 Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 20 Esta norma complementar deve ser revisada a cada 12 meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação do Comitê Gestor de Segurança da Informação.

Art. 21 A STIC deverá informar ao Gestor de Segurança da Informação, no prazo de 120 dias, quais ativos de informação que não puderam se adequar a esta norma.

Art. 22 Esta Instrução Normativa entra em vigor na data de sua publicação.

Cientifique-se. Publique-se. Cumpra-se.

Mario Lobão Carvalho
Diretor-Geral

São Luís, 05 de junho de 2024.

Documento assinado eletronicamente por **MARIO LOBÃO CARVALHO**, **Diretor Geral**, em 05/06/2024, às 16:54, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ma.jus.br/autenticar informando o código verificador **2177154** e o código CRC **60A8DAFA**.

0010062-96.2023.6.27.8000	2177154v6

Criado por 032165741198, versão 6 por 032165741198 em 05/06/2024 14:29:27.