Tribunal Regional Eleitoral - RJ
Diretoria Geral
Secretaria de Administração
Coordenadoria de Gestão Documental, Informação e Memória

INSTRUÇÃO NORMATIVA DG TRE-RJ Nº 13, DE 22 DE DEZEMBRO DE 2022.

Dispõe sobre as regras e os procedimentos para o uso de recursos criptográficos no Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das suas atribuições legais e regimentais,

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

CONSIDERANDO a **Resolução CNJ n.º 396, de 7 de junho de 2021 (https://atos.cnj.jus.br/atos/detalhar/3975)**, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a **Resolução TSE n.º 23.644, de 1º de julho de 2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e 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 n.º 13.709, de 14 de agosto de 2018 (LGPD) (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)**;

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 Rio de Janeiro; e

CONSIDERANDO, ainda, o disposto no processo SEI n.º 2022.0.000055706-5,

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a norma para o uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro.

Art. 2° Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela **Res. TSE n.º 23.644/2021 (https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021)**.

Art. 3° Para efeitos desta norma consideram-se os termos e definições previstos na **Portaria DG /TSE n.º 444/2021 (https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-444-de-08-de-julho-de-2021)**.

CAPÍTULO II

DO OBJETIVO

Art. 4° 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. 5° 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. 6° Toda comunicação cliente/servidor onde trafeguem dados pessoais ou logins e senhas, deve utilizar protocolos de comunicação segura.

CAPÍTULO IV

DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS

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

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

Art. 9° Os notebooks e dispositivos móveis de propriedade da Justiça Eleitoral devem ter seus discos rígidos protegidos por criptografia, visando diminuir o risco de vazamento de dados em caso de roubo, furto ou perda.

CAPÍTULO V

DA ASSINATURA DIGITAL

Art. 10. A Secretaria de Tecnologia da Informação (STI) 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-RJ 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) autoassinada.

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 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 Assessoria da Segurança da Informação e a Comissão de Segurança da Informação sobre eventuais não-conformidades.

Art. 15. Cabe ao usuário:

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

II - informar imediatamente à STI em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação;

III - ter ciência de que a assinatura ou login feitos por meio de certificado digital são irretratáveis, não podendo alegar que não efetuou a ação.

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 ser imediatamente submetida à Assessoria de Segurança da Informação para manifestação e posterior encaminhamento para apreciação pela Comissão de Segurança da Informação.

Art. 17. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida, se necessário, a Comissão de Segurança da Informação.

Art. 18. Esta norma deve ser revisada a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação com participação da Secretaria de Tecnologia da Informação e posterior encaminhamento para apreciação pela Comissão de Segurança da Informação.

Art. 19. Esta norma entra em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data, com exceção do disposto no artigo 9º, cuja implementação ocorrerá no prazo de 24 (vinte e quatro) meses.

ELINE IRIS RABELLO GARCIA DA SILVA

Diretora-Geral

Este texto não substitui o publicado no **DJE TRE-RJ nº 01, de 02/01/2023, p. 2 (https://dje.tse.jus.br/dje/pdf/v1/edicao/101323#page=2)**