**TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE**
**GABINETE DA PRESIDÊNCIA**

# PORTARIA Nº 241/2023 - GP

Dispõe sobre o uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE, no uso das atribuições que lhe são conferidas pelo artigo 20, inciso XIX, da Resolução nº 09/2012 - TRE/RN, e

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

CONSIDERANDO a Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TSE nº 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-RN nº 110/2023, que institui a Política de Segurança da Informação (PSI), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte;

CONSIDERANDO a Portaria DG TSE nº 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas à Política de Segurança da Informação do Tribunal Superior Eleitoral;

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

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei nº 13.709, de 14 de agosto de 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 de Rio Grande do Norte;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8, e tendo em vista o que consta no Processo PAE nº 10.487/2023;

RESOLVE:

## CAPÍTULO I
## DISPOSIÇÕES PRELIMINARES

Art. 1º O uso de recursos criptográficos, no âmbito do Tribunal, observará as disposições contidas nesta portaria.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução 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 nº 444/2021.

## CAPÍTULO III
## DO OBJETIVO

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 IV
## 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 V
## DA CRIPTOGRAFIA DOS DADOS ARMAZENADOS

Art. 7º Os dados pessoais sensíveis armazenados em servidores e bancos de dados devem adotar técnicas de criptografia, 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 *notebooks* e dispositivos móveis, de propriedade da Justiça Eleitoral, utilizados em trabalho remoto e teletrabalho, devem ter seus discos rígidos protegidos por criptografia, visando diminuir o risco de vazamento de dados em caso de furto.

## CAPÍTULO VI
## DA ASSINATURA DIGITAL

Art. 10. A Secretaria de Tecnologia da Informação e Eleições (STIE) 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 VII
## DA AUTORIDADE CERTIFICADORA

Art. 12. O Tribunal Regional Eleitoral do Rio Grande do Norte 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 VIII
## DAS RESPONSABILIDADES

Art. 14. Cabe à Comissão Permanente de Segurança da Informação (CPSI):

I - propor recursos necessários à implementação das ações de segurança da informação; e

II - propor a realização de análise de riscos.

Art. 15. Cabe à Secretaria de Tecnologia da Informação e Eleições (STIE), 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; e

V - informar ao Comitê Gestor de Segurança da Informação eventuais não conformidades.

Art. 16. 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 Secretaria de Tecnologia da Informação e Eleições (STIE) em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação; e

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.

## CAPÍTULO IX
## DISPOSIÇÕES FINAIS

Art. 17. 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, formalizado pela unidade técnica responsável, sendo imediatamente submetido para apreciação ao Gestor de Segurança da Informação.

Art. 18. Os casos omissos serão resolvidos pela Comissão Permanente de Segurança da Informação (CPSI).

Art. 19. A Secretaria de Tecnologia da Informação e Eleições (STIE) elaborará, em até 120 (cento e vinte) dias, os procedimentos operacionais para aplicação desta norma, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.

Art. 20. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 21. Esta norma deve ser revisada a cada 12 (doze) meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação da Comissão Permanente de Segurança da Informação (CPSI).

Art. 22. A Secretaria de Tecnologia da Informação e Eleições (STIE) deverá informar ao Gestor de Segurança da Informação, no prazo de 12(doze) meses, quais ativos de informação não puderam se adequar a esta norma.

Art. 23. Esta portaria entra em vigor na data de publicação e sua implementação se fará no prazo de 12 (doze) meses a contar desta data, com exceção do disposto no artigo 9º, cuja implementação ocorrerá no prazo de 24 (vinte e quatro) meses.

Natal/RN 12 de dezembro de 2023.

Desembargador **Cornélio Alves**
Presidente