TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Portaria Presidência Nº 77/2023 TRE/PRESI/DG/ASSDG, de 13 de fevereiro de 2023

Dispõe sobre a regulamentação do uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais,

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

CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a Lei nº 13.709/2018 (LGPD);

CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução nº 448, de 24 de maio de 2022, que adota a PSI da Justiça Eleitoral estabelecida pela citada Resolução nº 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral;

CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013;

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

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 Piauí;

RESOLVE:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída, por meio deste normativo, a regulamentação do uso de recursos criptográficos no âmbito do Tribunal Regional Eleitoral do Piauí.

Art. 2º Esta norma integra a Política de Segurança de Informação da Justiça Eleitoral, estabelecida pela Resolução nº 448, de 24 de maio de 2022.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos desta norma consideram-se os termos e definições a

seguir:

I - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

II - Assinatura digital: tipo de assinatura eletrônica que usa operações matemáticas com base em algoritmos criptográficos, de criptografia assimétrica, para garantir segurança quanto a autenticidade das documentações. Para assinar digitalmente um documento é necessário possuir um certificado digital. Entre as principais vantagens do uso de assinatura digital estão o não repúdio e tempestividade;

III - Atividades críticas: atividades precípuas da Justiça Eleitoral cuja interrupção ocasiona severos transtornos, como por exemplo: perda de prazos administrativos e judiciais, danos à imagem institucional, prejuízo ao erário, entre outros;

IV - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

V - Ativo de informação: patrimônio composto por todos os dados e informações gerados, adquiridos, utilizados ou armazenados pela Justiça Eleitoral;

VI - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

VII - Autenticidade: propriedade que garante que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VIII - Ciclo de vida da informação: ciclo formado pelas fases de produção, recepção, organização, uso, disseminação e destinação;

IX - Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro por outros ininteligíveis a pessoas não autorizadas a conhecê-los;

X - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

XI - Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

XII - Disponibilidade: propriedade da informação que garante que ela será acessível e utilizável sempre que demandada;

XIII - Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XIV - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

XV - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XVI - Integridade: propriedade que garante que a informação mantém

todas as características originais estabelecidas pelo proprietário;

XVII - Irretratabilidade (ou não repúdio): garantia de que a pessoa se responsabilize por ter assinado ou criado a informação;

XVIII - Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

XIX - Recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XX - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXI - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

XXII - Registro de eventos (log): processo com a finalidade de registrar eventos durante o seu ciclo de vida, podendo ser gerado por sistemas operacionais, aplicações, entre outros, e armazenado durante um período pré-determinado;

XXIII - Resumo criptográfico: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor - conhecida como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável, ou seja, utilizando-se apenas o *hash* não é possível recuperar a mensagem que o gerou;

XXIV - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XXV - Segurança da informação: abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos princípios da autenticidade, da confidencialidade, da integridade, da disponibilidade e da irretratabilidade da informação, entre outras propriedades;

XXVI - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXVII - Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXVIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

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 trafeguem 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, notebooks e dispositivos móveis, 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 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 adotando os procedimentos técnicos cabíveis.

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-PI 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 Comissão 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 STI 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.

CAPÍTULO VIII

DAS 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 da Comissão de Segurança da Informação.

Art. 17. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 18. A STI elaborará, em até 180 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 Núcleo de Segurança da Informação, com consequente adoção das providências cabíveis.

Art. 20. Esta Portaria deve ser revisada a cada 12 meses pelo Núcleo de Segurança da Informação e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 21. A STI deverá informar ao Núcleo de Segurança da Informação, no prazo de 180 dias, quais ativos de informação que não puderam se adequar a esta norma.

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

Desembargador ERIVAN LOPES

Presidente do TRE-PI

Documento assinado eletronicamente por **Erivan José da Silva Lopes**, **Presidente**, em 13/02/2023, às 09:58, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.