



TRIBUNAL REGIONAL ELEITORAL DO PARÁ

INSTRUÇÃO NORMATIVA Nº 1, DE 07 JANEIRO DE 2021

Dispõe sobre a emissão, revogação e utilização de certificados digitais no âmbito do Tribunal Regional Eleitoral do Pará.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ, no uso de suas atribuições e tendo em vista o Processo Administrativo Eletrônico protocolado sob o n.º 0000145-84.2021.6.14.8000,

CONSIDERANDO a utilização de certificados digitais e assinaturas digitais no processo judicial eletrônico;

CONSIDERANDO a necessidade de regulamentar as atividades relativas ao uso e à distribuição de certificados digitais no âmbito do Tribunal Regional Eleitoral do Pará;

CONSIDERANDO a necessidade de racionalizar a concessão de certificados digitais institucionais, de modo a zelar pela economia de recursos públicos em prestígio aos princípios que regem a administração pública;

CONSIDERANDO a necessidade de sensibilização quanto aos efeitos legais decorrentes do uso do certificado digital para produção de assinaturas digitais; e

CONSIDERANDO a necessidade de promover a confidencialidade e integridade das informações no âmbito deste Tribunal;

RESOLVE:

Art. 1º Estabelecer a norma para a utilização de certificados digitais no âmbito do Tribunal Regional Eleitoral do Pará.

Art. 2º Esta Norma integra a estrutura normativa da Segurança da Informação deste Tribunal, instituída por meio do Art. 8º da Resolução TRE-PA 5.430/2018, de 27 de março de 2018.

CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES

Art. 3º Para efeitos desta Norma, aplicam-se as seguintes definições:

I. sistemas e serviços de informação: qualquer software, desenvolvido ou não no âmbito do Tribunal, que acesse e/ou manipule informações relacionadas às atividades da instituição;

II. identidade: conjunto de atributos (lógicos e/ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação. Exs.: login e senha, certificado digital e senha, características biométricas, etc;

III. Autoridade Certificadora (AC): entidade responsável pelo processo de emissão, renovação e revogação de certificados digitais válidos;

IV. certificado digital: documento eletrônico, emitido por uma Autoridade Certificadora confiável, o qual

identifica univocamente uma pessoa física, uma pessoa jurídica ou um computador;

V. assinatura digital: método de autenticação de documentos digitais, com valor jurídico semelhante à assinatura física em papel;

VI. unidade administrativa: unidade do Tribunal à qual se atribuiu a responsabilidade pela gestão da certificação digital;

VII. documento eletrônico: documento cujas informações são armazenadas exclusivamente em meios eletrônicos;

VIII. assinatura digital: instrumento que permite a autenticação da autoria e a garantia da integridade de mensagens, documentos ou transações eletrônicas com base em mecanismos criptográficos;

IX. Certificado Digital: documento eletrônico emitido por autoridade certificadora, que contém, entre outras informações, a identificação de seu titular, acompanhado de um par de chaves criptográficas utilizadas no processo de assinatura digital, além de outras funcionalidades. A legislação vigente confere validade jurídica aos atos praticados por meio do certificado digital emitido por autoridade certificadora vinculada à ICP-Brasil, tal como a assinatura digital;

X. mídia criptográfica: dispositivo de hardware criptográfico utilizado para armazenar o certificado digital. Os certificados digitais institucionais no âmbito da Justiça Eleitoral são armazenados e disponibilizados em mídias do tipo cartão inteligente (*smart card*) ou *token*;

XI. Infraestrutura de Chaves Públicas Brasileira – (ICP-Brasil): infraestrutura constituída por conjunto de técnicas, práticas e procedimentos que visam à realização de transações eletrônicas seguras, bem como à garantia da autenticidade, da integridade e da validade jurídica de documentos eletrônicos que utilizam certificados digitais;

XII. Autoridade Certificadora – AC: entidade subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais, entre outras atividades;

XIII. AC-JUS: autoridade certificadora da Justiça que integra a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil como autoridade certificadora de primeiro nível;

XIV. Cert-JUS: certificado digital emitido sob a cadeia da AC-JUS, destinado aos órgãos do Poder Judiciário e da administração pública direta e indireta, que identifica o usuário por suas informações pessoais e funcionais;

XV. Cert-JUS Institucional: certificado digital destinado exclusivamente aos usuários internos do Poder Judiciário, emitido mediante autorização formal da instituição, o qual contém as informações pessoais e funcionais do seu titular;

XVI. Certificado tipo A3: tipo de certificado que utiliza dispositivo criptográfico para gerar e armazenar o par de chaves associado, destinado à identificação de pessoas físicas e jurídicas, com validade máxima de cinco anos;

XVII. PIN (*Personal Identification Number*): senha alfanumérica destinada à utilização do certificado digital, a qual, se digitada erroneamente um determinado número de vezes, bloqueará o certificado;

XVIII. PUK (*Personal Identification Number Unblocking Key*): senha alfanumérica destinada exclusivamente para o desbloqueio do PIN, a qual, se digitada erroneamente um determinado número de vezes, inutilizará o certificado;

XIX. Autoridade de Registro – AR: entidade credenciada pela AC Raiz e sempre vinculada operacionalmente a uma determinada autoridade certificadora, responsável por identificar e cadastrar os usuários e encaminhar as solicitações de certificados digitais à AC;

XX. Chave Privada: é a chave secreta de um certificado digital, de acesso protegido por senha, empregada no processo de assinatura digital;

XXI. Chave Pública: é a chave de conhecimento público de um certificado digital, utilizada para verificar uma assinatura digital;

XXII. Senha de Emissão: é a senha informada pelo solicitante durante a etapa de solicitação do certificado digital e requerida durante o processo de sua emissão;

XXIII. Senha de Revogação: é a senha utilizada pelo titular do certificado para revogá-lo, sem a necessidade de comparecer à autoridade de registro;

XXIV. Revogação: procedimento por meio do qual o titular do certificado digital solicita à autoridade certificadora a sua anulação, tornando sem validade jurídica os atos praticados com este certificado após a data da revogação;

XXV. Renovação: procedimento por meio do qual o titular do certificado digital solicita à autoridade certificadora, antes da expiração de sua validade, a prorrogação da vigência do certificado digital emitido de forma presencial, por igual período de validade, dispensada a exigência de comparecimento do titular à autoridade de registro para validação dos documentos apresentados quando da emissão do certificado. O procedimento de renovação é limitado a uma ocorrência após a emissão de um certificado novo com validação presencial.

Art. 4º As disposições desta Norma aplicam-se a todos os usuários de recursos de tecnologia da informação do Tribunal Regional Eleitoral do Pará, conforme disposto no artigo 5º da Política de Segurança da Informação, devendo ser rigorosamente observadas sob pena de responsabilidade.

CAPÍTULO II DO CERTIFICADO DIGITAL

Art. 5º O certificado digital será utilizado pelo usuário interno do TRE-PA na prática de atos que exijam sua identificação funcional e pessoal em meio eletrônico.

§ 1º O certificado digital a que se refere o caput deverá ser o de perfil “Institucional” pertencente à cadeia “Cert-JUS”, e do tipo A3 ou superior quanto aos requisitos de segurança.

§ 2º O certificado digital é de uso pessoal, intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado, nos termos da legislação em vigor.

§ 3º A prática de atos assinados eletronicamente importará na aceitação das normas regulamentares sobre o tema e na responsabilização pela utilização indevida da assinatura eletrônica.

§ 4º A utilização do certificado digital para qualquer operação implicará o não repúdio e impedirá o titular de negar a autoria da operação ou de alegar que ela tenha sido praticada por terceiro.

§ 5º O não repúdio referido no parágrafo anterior aplica-se, também, às operações efetuadas entre o período de solicitação de revogação e a respectiva inclusão na lista de certificados revogados, publicada pela autoridade certificadora.

§ 6º O uso inadequado do certificado digital, a recusa de utilização deste instrumento na prática de atos que requeiram seu uso ou a não adoção das providências necessárias à manutenção da validade do certificado digital ficarão sujeitos à apuração de responsabilidade administrativa.

CAPÍTULO III DA EMISSÃO DE CERTIFICADO DIGITAL

Art. 6º O processo de emissão do certificado digital é composto pelas etapas de solicitação, validação presencial e gravação do certificado digital em mídia apropriada.

§ 1º A solicitação de certificado digital deverá ser precedida de permissão da autoridade competente, considerada esta a autoridade máxima do órgão, o representante legal do órgão ou outra pessoa expressamente designada para esta finalidade, a qual ficará responsável pela exatidão das informações fornecidas para emissão do certificado, de acordo com a política da autoridade certificadora.

§ 2º As etapas de solicitação e validação presencial deverão observar as regras estabelecidas pela autoridade certificadora responsável pela emissão do certificado.

§ 3º A gravação do certificado digital na mídia é a etapa que encerra o processo de emissão e consiste na geração e armazenamento dos dados que compõem o certificado.

§ 4º Superada a etapa de gravação, o titular do certificado digital deverá informar as datas de início e fim de sua validade à unidade administrativa competente.

CAPÍTULO IV DA REVOGAÇÃO DE CERTIFICADO DIGITAL

Art. 7º A revogação do certificado digital deverá ser solicitada pelo titular do certificado:

- I. se ocorrer perda, roubo, furto, extravio e inutilização da mídia;
- II. se houver alteração de qualquer informação contida no certificado;
- III. se ocorrer comprometimento ou suspeita de comprometimento de sua chave privada;
- IV. se não mais fizer parte do quadro de pessoal do Tribunal.

Art. 8º A Secretaria de Tecnologia da Informação poderá solicitar a revogação do certificado digital, nos casos de:

- I. perda da necessidade de utilização do serviço;
- II. licenças e afastamentos temporários sem remuneração;
- III. identificação de vulnerabilidade, risco à segurança da Rede do Tribunal ou uso indevido no serviço concedido;

Parágrafo único. É obrigatória a solicitação da revogação do certificado digital quando o usuário interno não estiver mais vinculado ao quadro de pessoal do Tribunal.

Art. 9º A solicitação de revogação do certificado digital deverá ser realizada conforme procedimentos da autoridade certificadora que o emitiu.

Parágrafo único. Caso o pedido seja apresentado pelo titular do certificado, este deverá comunicar à Secretaria de Tecnologia da Informação a razão de sua solicitação.

CAPÍTULO V DA RENOVAÇÃO DE CERTIFICADO DIGITAL

Art. 10. A renovação do certificado digital deverá ser realizada dentro do prazo de validade do certificado digital, em período não superior a 30 dias da data de expiração do certificado.

Parágrafo único. Após a renovação do certificado digital, o seu titular deverá informar as novas datas de validade à unidade administrativa competente, conforme estabelecido no § 4º do art. 6º.

CAPÍTULO VI DAS OBRIGAÇÕES DO TITULAR DE CERTIFICADO DIGITAL

Art. 11. São obrigações dos titulares de certificado digital:

- I. fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação na fase de solicitação do certificado, de acordo com as normas da autoridade certificadora;
- II. apresentar tempestivamente à autoridade certificadora a documentação necessária à emissão do certificado digital;
- III. garantir a proteção e o sigilo de sua chave privada, do PIN, do PUK e das senhas de revogação e emissão;
- IV. zelar pela proteção, guarda e integridade da mídia onde se encontra armazenado o certificado digital;
- V. estar sempre de posse do certificado digital para o desempenho de atividades profissionais que

requeiram o seu uso;

VI. utilizar o seu certificado de modo apropriado, conforme legislação aplicável, incluindo as políticas da autoridade certificadora emissora do certificado;

VII. verificar, no momento da emissão do certificado, a veracidade e exatidão das informações nele contidas e notificar a autoridade certificadora em caso de inexatidão ou erro;

VIII. solicitar imediata revogação do certificado nos casos previstos no Art. 7º;

IX. devolver à unidade administrativa competente a mídia do seu certificado digital em até 10 dias úteis após sua revogação, expiração ou desligamento do quadro funcional.

Art. 12. Caberá ao titular do certificado digital acionar a Central de Serviços de TI para solução de problemas.

CAPÍTULO VII DAS ATRIBUIÇÕES INSTITUCIONAIS

Art. 13. Caberá à Secretaria de Tecnologia da Informação:

I. prover, no que couber, os recursos necessários à emissão, renovação, revogação e utilização dos certificados digitais;

II. desenvolver atividades para orientar e conscientizar seus usuários internos, em relação aos aspectos operacionais e de segurança no uso dos certificados digitais;

III. fornecer pelo menos 1 (um) certificado digital para cada usuário interno do PJe, substituindo-os no prazo mínimo de 15 (quinze) dias antes da expiração da validade e imediatamente nos casos de defeitos que impeçam a utilização;

IV. adequar a infraestrutura de TI para uso dos certificados digitais;

V. adotar as providências para a instalação dos softwares e equipamentos necessários à utilização dos certificados digitais;

VI. atender as demandas geradas pelo titular do certificado digital sobre problemas e incidentes técnicos ocorridos no tempo de vigência do certificado;

VII. prestar suporte e dirimir as dúvidas dos usuários internos sobre questões técnicas.

VIII. adotar medidas para controle de entrega e substituição dos certificados digitais que fornecerem aos usuários internos, adotando providências necessárias à substituição independente de requerimento ou manifestação do usuário.

Art. 14. Competirá à unidade administrativa responsável pelas informações funcionais dos usuários internos do respectivo órgão:

I. gerenciar o processo de contratação de mídias e certificados digitais;

II. promover o levantamento da necessidade de aquisições de mídias e certificados digitais;

III. programar as visitas do agente da autoridade de registro (AR) às dependências do Tribunal para validação presencial, quando houver previsão contratual;

IV. monitorar os prazos de expiração dos certificados digitais em vigor;

V. fiscalizar a execução do contrato associado aos certificados digitais em uso pelo Tribunal.

CAPÍTULO VIII DOS CUSTOS DE EMISSÃO E RENOVAÇÃO DE CERTIFICAÇÃO DIGITAL

Art. 15. Os custos de emissão e renovação do certificado digital, para uso institucional dos usuários internos do Tribunal, correrão por conta da ação “20GP”, PTRES 067602, Elemento de Despesa 3390.39 -

Outros Serviços de terceiros PJ.

Art. 16. O titular de certificado digital solicitado, emitido ou renovado, às expensas do Tribunal Regional Eleitoral do Pará, deverá custear a emissão de novo certificado ou ressarcir o erário, em quaisquer das hipóteses abaixo, desde que implique em ônus adicional para o órgão:

- I. perda do prazo fixado pela autoridade certificadora para emissão do certificado digital;
- II. não renovação do certificado digital dentro do seu prazo de validade;
- III. renovação do certificado digital em desconformidade com o art. 10, pelo valor proporcional ao tempo restante de validade do certificado;
- IV. perda, extravio ou dano da mídia que resulte na inoperância do certificado digital, pelo valor proporcional ao tempo restante de validade do certificado;
- V. inutilização do certificado digital em razão de esquecimento da senha de utilização (PIN) ou de desbloqueio (PUK), pelo valor proporcional ao tempo restante de validade do certificado.

Parágrafo único. No caso de furto ou roubo do dispositivo, o titular estará dispensado da obrigação disposta no caput, desde que apresente registro de ocorrência policial ou declaração com a descrição da ocorrência.

CAPÍTULO IX DAS DISPOSIÇÕES FINAIS

Art. 17. Os casos omissos serão submetidos à deliberação da Comissão de Segurança da Informação.

Art. 18. A presente Norma entra em vigor a partir da data de sua publicação.

Belém, 07 de janeiro de 2021.



Documento assinado eletronicamente por **EDUARDO SOUSA DE ARAÚJO**, **Diretor Geral substituto**, em 11/01/2021, às 13:19, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1213991** e o código CRC **BF6E67FB**.