DECLARAÇÃO DE PRÁTICAS DE NEGÓCIOS DA AUTORIDADE DE REGISTRO

AR PRODESP

VINCULADA A AC PRODESP e AC PRODESP RFB

Versão 1.0

18 de novembro de 2021

1. INTRODUÇÃO

1.1 VISÃO GERAL

Este documento descreve as práticas e procedimentos comerciais realizados por essa Autoridade de Registro, vinculada a AC PRODESP AC PRODESP RFB, integrante da Infraestrutura de Chaves Públicas Brasileiras da ICP-Brasil.

Esta DPN está alinhada com a Declaração de Práticas de Certificação (DPC), Política de Certificados (PC) e Política de Segurança da AC PRODESP e AC PRODESP RFB e aos *Princípios e Critérios WebTrust para AR (WebTrust Principles and Criteria for Registration Autorities).*

A **AR PRODESP** mantém todas as informações da sua DPN sempre atualizadas.

1.2 NOME DO DOCUMENTO E PUBLICAÇÃO

Este documento é chamado "Declaração de Práticas de Negócio da **AR IMESP**, referido a seguir simplesmente como **DPN** – **AR PRODESP** e descreve as práticas e os procedimentos comerciais empregados por essa AR. Este documento é divulgado à AC PRODESP e AC PRODESP RFB.

1.3 HIERARQUIA

A **AR PRODESP** está vinculada à Autoridade Certificadora PRODESP RFB que por sua vez está subordinada à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC RFB) e a Autoridade Certificadora PRODESP, que está subordinada a AC PRODESP SP subordinadas hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).

1.4 TIPOS DE CERTIFICADOS

Com relação aos tipos específicos de certificados emitidos pela AR **AR PRODESP**, devem ser observadas as Políticas de Certificado (PC) publicadas na página web https://certificadodigital.imprensaoficial.com.br/repositorio/ que explicam como os certificados são gerados, administrados pela AC PRODESP e AC PRODESP RFB e utilizados pela comunidade.

As Políticas de Certificados praticadas por esta AR são:

- PC A1

- PC A3
- PC A4

2. IDENTIFICAÇÃO E AUTENTICAÇÃO

Esta AR verifica a autenticidade da identidade de pessoas físicas e jurídicas titulares de certificados.

O procedimento de identificação do titular do certificado é realizado mediante a presença física do interessado ou por videoconferência conforme o caso, com base nos documentos oficiais de identificação apresentados.

2.1 IDENTIFICAÇÃO DE UM INDIVÍDUO

Deve ser comprovado que a pessoa que se apresenta como titular do certificado pessoa física é realmente aquela cujos dados constam no documento de identificação pessoal apresentado.

Além da identificação por base nos documentos pessoais, o requerente do certificado deve ser submetido a coleta das impressões digitais e captura da face para a identificação biométrica.

A identificação biométrica na ICP-Brasil é obrigatória.

Os documentos pessoais aceitos para emissão do certificado devem ser apresentados em sua versão original oficial, podendo ser físico ou digital. São eles:

a) Registro de Identidade ou Passaporte, se brasileiro;
b) Título de Eleitor, com foto;
c) Carteira Nacional de Estrangeiro, se estrangeiro domiciliado no Brasil
d) Passaporte se estrangeiro não domiciliado no Brasil;

Nota 1: Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação especifica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

Nota 2: Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos.

Na hipótese das biometrias do titular já estarem cadastradas na base da ICP-Brasil, e houver parecer positivo ao realizar a identificação biométrica, fica dispensada a apresentação dos documentos acima e o certificado poderá ser liberado para emissão.

2.2 IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

Para o titular pessoa jurídica, será designada pessoa física como responsável pelo uso do certificado, que será a detentora da chave privada.

Deve ser comprovado que a pessoa que se apresenta como titular do certificado é o responsável legal pela organização e que possui tal atribuições admitida a procuração.

Os documentos aceitos para confirmar a identidade da pessoa jurídica são:

a) Relativos à sua habilitação jurídica:

i. Se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;

ii. Se entidade privada:

1. Certidão simplifica emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
2. Documento da eleição de seus representantes legais, quando aplicável;

b) Relativos a sua habilitação fiscal:
i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

ii. prova de inscrição no Cadastro Específico do INSS – CEI.

NOTA 1: Essas confirmações poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

2.3 EMISSÃO DO CERTIFICADO

Após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados, na etapa de identificação, é liberada a emissão do certificado no sistema da AC. A extensão Subject Alternative Name é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

2.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES ANTES DA EXPIRAÇÃO

Um novo certificado poderá ser requerido pelo solicitante antes da expiração de seu certificado vigente, no qual deverá enviar à AC PRODESP e AC PRODESP RFB uma solicitação, por meio eletrônico, assinada digitalmente com o uso de um certificado de assinatura digital de mesmo nível de segurança do certificado a ser renovado.

O processo de identificação e autenticação para rotinas de novas chaves antes da

expiração poderá ser conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;

b) a solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;

d)) solicitação por meio eletrônico dada nas alíneas 'b' e 'c', acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação editada pela AC Raiz ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;

e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico;

3. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

3.1 SOLICITAÇÃO DO CERTIFICADO

Os requisitos e procedimentos para solicitação de emissão do certificado por esta AR são:

a. Confirmação da identidade da pessoa física ou jurídica titular do certificado, conforme item 2 e seus subitens;
b. Termo de Titularidade assinado digitalmente pelo titular ou responsável pelo uso do certificado;
c. Autenticação biométrica do Agente de Registro responsável pela identificação e verificação do certificado.
d. Para a validação por videoconferência, o agente de registro se utilizará de um

serviço web para se autenticar e encaminhar ao solicitante do certificado o código OTP e o link para a videoconferência.

3.2 PARA GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular for uma pessoa jurídica, este indicará por seu representante legal no momento da emissão, a pessoa responsável pela geração e uso do certificado.

O armazenamento do certificado deverá obedecer a Política de Certificado correspondente, sendo:

Tipo do certificado	Mídia armazenadora
A1	Repositório protegido por senha e/ou identificação biométrica
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO

3.3 REVOGAÇÃO DO CERTIFICADO DIGITAL

O titular do certificado pode solicitar a revogação do seu certificado em qualquer tempo e independentemente de qualquer circunstância.

3.3.1 Circunstância para revogação

A revogação poderá ser feita pelos seguintes motivos:

a) Quando constatada emissão imprópria ou defeituosa;
b) Quando for necessária a alteração de qualquer informação constante no certificado;
c) No caso de comprometimento da chave privada correspondente ou da mídia armazenadora;
d) Por determinação judicial;
e) Por razões comerciais;
f) Risco de fraude.

3.3.2. Quem pode solicitar revogação

A solicitação de revogação de um certificado somente poderá ser feita:

g) Por solicitação do titular do certificado;
h) Por solicitação do responsável pelo certificado, no caso de certificado de pessoas jurídicas;
i) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
j) Por determinação da AC;
k) Por determinação da AR;
l) Por determinação do Comitê Gestor da ICP-Brasil ou da AC Raiz.

3.3.3 Procedimentos para solicitação de revogação

- O solicitante da revogação de um certificado deve ser identificado;
- A solicitação de revogação é feita através de um formulário específico, permitindo a identificação inequívoca do solicitante;
- O procedimento para revogação do certificado pode ser realizado por todos os Agentes de Registros habilitados na AR;
- As solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
- As justificativas para a revogação de um certificado são documentadas;
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4. OBRIGAÇÕES DA AR

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC RESPONSAVEL utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC RESPONSAVEL e pela ICP-Brasil, em especial com o contido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil, bem como Princípios e Critérios WebTrust para AR [5];
f) manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2,3.2.3 e 3.2.7;e
h) divulgar suas práticas, relativas à cadeia de AC ao qual se vincular, em conformidade com o documento princípios e Critérios Web Trust para AR [5].

.

5. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

6. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são encontrados no site oficial do ITI (http://www.iti.gov.br) e podem ser alterados, quando necessário, pelos órgãos competentes.

- [1] CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL- DOC-ICP-03.01;
- Declaração de Práticas de Certificação (DPC) da AC PRODESP;
- Política de Certificado (PC) do tipo A1 da AC PRODESP;
- Política de Certificado (PC) do tipo A3 da AC PRODESP;
- Política de Segurança (PS) da AC PRODESP;
- Declaração de Práticas de Certificação (DPC) da AC PRODESP RFB;
- Política de Certificado (PC) do tipo A1 da AC PRODESP RFB;
- Política de Certificado (PC) do tipo A3 da AC PRODESP RFB;
- Política de Segurança (PS) da AC PRODESP RFB;

7. REFERÊNCIAS BIBLIOGRÁFICAS

[2] PRINCÍPIOS E CRITÉRIOS WEBTRUST PARA AR (*WebTrust Principles and Criteria for Registration Authorities*), disponível em http://www.webtrust.org.