

**Política de Certificado de Assinatura Digital**  
**Tipo A1**  
**AC CNDL RFB**

Versão 3.1 Agosto/ 2020

## Contents

INTRODUÇÃO .....	5
1.1 VISÃO GERAL .....	5
1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO .....	5
1.3 PARTICIPANTES DA ICP-BRASIL.....	6
1.4. USABILIDADE DO CERTIFICADO.....	7
1.5 POLÍTICA DE ADMINISTRAÇÃO .....	7
1.6. DEFINIÇÕES E ACRÔNIMOS .....	8
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO.....	10
2.1. REPOSITÓRIOS .....	10
2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS.....	10
2.3. TEMPO OU FREQUÊNCIA DA PUBLICAÇÃO.....	10
2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS .....	10
3. IDENTIFICAÇÃO E AUTENTICAÇÃO .....	10
3.1. NOMEAÇÃO .....	10
3.2. VALIDAÇÃO INICIAL DE IDENTIDADE.....	10
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES .....	11
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO.....	11
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO .....	11
4.1. SOLICITAÇÃO DE CERTIFICADO .....	11
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO .....	11
4.3. EMISSÃO DE CERTIFICADO .....	11
4.4. ACEITAÇÃO DE CERTIFICADO .....	11
4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO.....	11
4.6. RENOVAÇÃO DE CERTIFICADOS.....	11
4.7. NOVA CHAVE DE CERTIFICADO.....	12
4.8. MODIFICAÇÃO DE CERTIFICADO.....	12
4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO.....	12
4.10 SERVIÇOS DE STATUS DE CERTIFICADO .....	13
4.11 ENCERRAMENTO DE ATIVIDADES .....	13
4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVE.....	13
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	13
5.1. CONTROLES FÍSICOS .....	13
5.2. CONTROLES PROCEDIMENTAIS.....	13
5.3. CONTROLES DE PESSOAL.....	14
5.4. PROCEDIMENTOS DE LOG DE AUDITORIA .....	14

5.5.	ARQUIVAMENTO DE REGISTROS.....	14
5.6.	TROCA DE CHAVE .....	14
5.7.	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE .....	14
5.8	EXTINÇÃO DE AC.....	15
6.	CONTROLES TÉCNICOS DE SEGURANÇA .....	15
6.1.	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	15
6.2.	PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO .....	17
6.3.	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES.....	18
6.4.	DADOS DE ATIVAÇÃO .....	19
6.5.	CONTROLES DE SEGURANÇA COMPUTACIONAL .....	19
6.6.	CONTROLES TÉCNICOS DO CICLO DE VIDA.....	20
6.7.	CONTROLES DE SEGURANÇA DE REDE .....	20
6.8	CARIMBO DO TEMPO.....	20
7.	PERFIS DE CERTIFICADO, LCR E OCSP .....	20
7.1.	PERFIL DO CERTIFICADO.....	20
7.2.	PERFIL DE LCR.....	27
7.3	PERFIL DE OCSP.....	28
8.	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES .....	28
8.1.	FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES .....	28
8.2.	IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR.....	28
8.3.	RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA.....	28
8.4.	TÓPICOS COBERTOS PELA AVALIAÇÃO .....	28
8.5.	AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	28
8.6.	COMUNICAÇÃO DOS RESULTADOS .....	28
9.	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	28
9.1.	TARIFAS.....	29
9.2.	RESPONSABILIDADE FINANCEIRA.....	29
9.3 .	CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO .....	29
9.4.	PRIVACIDADE DA INFORMAÇÃO PESSOAL.....	29
9.5.	DIREITO DE PROPRIEDADE INTELECTUAL .....	29
9.6.	DECLARAÇÕES E GARANTIAS .....	30
9.7.	ISENÇÃO DE GARANTIAS.....	30
9.8.	LIMITAÇÕES DE RESPONSABILIDADES .....	30
9.9.	INDENIZAÇÕES .....	30
9.10.	PRAZO E RESCISÃO.....	30

9.11.	AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES .....	30
9.12.	ALTERAÇÕES .....	30
9.13.	SOLUÇÃO DE CONFLITOS .....	31
9.14.	LEI APLICÁVEL .....	31
9.15.	CONFORMIDADE COM A LEI APLICÁVEL.....	31
9.16.	DISPOSIÇÕES DIVERSAS .....	31
9.17.	OUTRAS PROVISÕES.....	31
10.	DOCUMENTOS REFIRENCIADOS .....	31

**Autor:** Confederação Nacional de Dirigentes Lojistas - SPC Brasil

**Edição:** 17/08/2020

**Versão:** 3.1

## **INTRODUÇÃO**

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

### **1.1 Visão Geral**

**1.1.1.** Este documento descreve os requisitos mínimos para as Política de Certificado (PC) obrigatoriamente observado pela Autoridade Certificadora Confederação Nacional de Dirigentes Lojistas – SPC Brasil para assinatura digital tipo A1, integrantes da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

**1.1.2.** A Estrutura desta PC de assinatura digital tipo A1 da AC CDNL está baseada no documento Requisitos Mínimos para as Políticas de Certificados do Comitê Gestor da ICP-Brasil.

**1.1.3.** O tipo de certificado para usuários finais da ICP-Brasil emitidos pela AC CNDL descritos nesta esta PC é o Tipo A1.

**1.1.4.** Os tipos de certificados indicados acima, definem escalas de requisitos de segurança, nas quais o tipo A1 está associado aos requisitos menos rigorosos e o tipo A3 aos requisitos mais rigorosos.

**1.1.5.** Esta PC refere-se exclusivamente a certificados de pessoa física e de pessoa jurídica tipo A1, emitidos pela AC CNDL RFB.

**1.1.6.** Item não aplicável.

**1.1.7.** Item não aplicável.

**1.1.8.** Item não aplicável

**1.1.9.** Item não aplicável

**1.1.10.** Item não aplicável

### **1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO**

**1.2.1.** Esta PC é chamada de Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora CNDL RFB. O Object Identifier (OID) atribuído para a PC A1 da AC CNDL RFB é **2.16.76.1.2.1.52**.

**1.2.2.** Item não aplicável

### 1.3 PARTICIPANTES DA ICP-BRASIL

#### 1.3.1 AUTORIDADE CERTIFICADORA (AC)

**1.3.1.1.** Esta PC está relacionada à AC CNDL RFB integrante da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil, sob a hierarquia da Autoridade Certificadora RFB – AC RFB, que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira – AC Raiz.

**1.3.1.2.** As práticas e procedimentos de certificação da AC CNDL RFB estão descritos na Declaração de Práticas de Certificação da AC CNDL RFB a seguir designada simplesmente por "DPC-AC CNDL RFB".

A AC CNDL RFB mantém as informações acima sempre atualizadas.

#### 1.3.2 AUTORIDADES DE REGISTRO (AR)

**1.3.2.1.** A AC CNDL RFB informa que os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência das Autoridades de Registro - AR.

**1.3.2.2.** As Autoridades de Registro vinculadas (ARV) à AC CNDL RFB estão relacionadas na página Web:

<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

Os conteúdos relacionados na página Web <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital> são:

- a) Relação de todas as AR credenciadas
- b) Relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

A AC CNDL RFB mantém as informações acima sempre atualizadas.

#### 1.3.3 TITULARES DE CERTIFICADO

Os Titulares do Certificado de Assinatura Digital tipo A1 da AC CNDL RFB podem ser pessoas físicas ou jurídicas, desde que não estejam na situação cadastral CANCELADA ou NULA (pessoa física) ou INAPTA, SUSPENSA, BAIXADA ou NULA (pessoa jurídica). conforme o disposto nos incisos I e II do art. 6º da Instrução Normativa RFB nº 1077, de 29 de Outubro de 2010 e Anexo I da Portaria RFB/Sucor/Cotec nº 18, de 19 de fevereiro de 2019 (Leiute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 4.4).

**1.3.3.1.** A validação do nome e da situação cadastral do titular do certificado (e do responsável, quando for o caso), é realizada por intermédio do sistema Consulta Prévia, disponibilizado pela AC RFB às Autoridades Certificadoras Habilitadas.

**1.3.3.2.** No caso de certificado emitido para pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB.

#### **1.3.4. PARTES CONFIÁVEIS**

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

#### **1.3.5. OUTROS PARTICIPANTES**

Todos os Prestadores de Serviços de Suporte vinculados à AC CNDL RFB estão relacionados na página Web <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

### **1.4. USABILIDADE DO CERTIFICADO**

#### **1.4.1. USO APROPRIADO DO CERTIFICADO**

**1.4.1.1.** Os certificados definidos por esta PC possuem sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação, autenticação de seu titular.

**1.4.1.2.** As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

**1.4.1.3.** Na definição das aplicações para o certificado definido pela PC, a AC CNDL RFB considera-se o nível de segurança previsto para o tipo do certificado. Esse nível de segurança caracteriza-se pelos requisitos mínimos que são definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

**1.4.1.4.** Os certificados de tipo A1 emitidos pela AC CNDL RFB no âmbito desta PC podem ser utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

**1.4.1.5.** Item não aplicável.

**1.4.1.6.** Item não aplicável.

**1.4.1.7.** Item não aplicável.

**1.4.1.8.** Item não aplicável.

#### **1.4.2. USO PROIBITIVO DO CERTIFICADO**

**1.4.2.1** Item não aplicável.

### **1.5. POLÍTICA DE ADMINISTRAÇÃO**

#### **1.5.1. ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO**

Nome da AC: AC CNDL RFB

#### **1.5.2. CONTATO**

AC CNDL RFB

Rua: Leônicio de Carvalho nº 234 – 13º Andar

CEP: 04003-010

Paraiso - São Paulo, SP

Telefones: (55 11) 3549-6800 / 3003-0633  
Área para contato: Serviço de Atendimento ao Cliente.  
E-mail: [sac.cd@spcbrasil.org.br](mailto:sac.cd@spcbrasil.org.br)

### 1.5.3. PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Marli Paiva Rubio

Telefone: (11) 3549-6800

E-mail: [auditoriaecompliancecd@spcbrasil.org.br](mailto:auditoriaecompliancecd@spcbrasil.org.br)

Outros: Setor de Auditoria e Compliance

### 1.5.4. PROCEDIMENTOS DE APROVAÇÃO DA PC

Esta PC é aprovada pelo ITI. Os procedimentos de aprovação da PC da AC CNDL RFB são estabelecidos a critério do CG da ICP-Brasil.

### 1.6. DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
<i>CMM-SEI</i>	<i>Capability Maturity Model do Software Engineering Institute</i>
<i>CMVP</i>	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoa Jurídica
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas



CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments

RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

## **2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO**

Os itens seguintes estão referidos em seus correspondentes na DPC AC CNDL RFB.

### **2.1. REPOSITÓRIOS**

### **2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS**

### **2.3. TEMPO OU FREQUÊNCIA DA PUBLICAÇÃO**

### **2.4. CONTROLE DE ACESSO AOS REPOSITÓRIOS**

## **3. IDENTIFICAÇÃO E AUTENTICAÇÃO**

Os itens seguintes estão referidos nos correspondentes itens da DPC AC CNDL RFB.

### **3.1. NOMEAÇÃO**

#### **3.1.1. Tipos de nomes**

#### **3.1.2. Necessidade de nomes significativos**

#### **3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado**

#### **3.1.4. Regras para interpretação de vários tipos de nomes**

#### **3.1.5. Unicidade de nomes**

#### **3.1.6. Procedimento para resolver disputa de nomes**

#### **3.1.7. Reconhecimento, autenticação e papel de marcas registradas**

### **3.2. VALIDAÇÃO INICIAL DE IDENTIDADE**

#### **3.2.1. Método para comprovar a posse de chave privada**

#### **3.2.2. Autenticação da identidade de um indivíduo**

#### **3.2.3. Autenticação da identidade de equipamento ou aplicação**

#### **3.2.4. Informações não verificadas do titular do certificado**

3.2.5. Autenticação da identidade de uma organização

3.2.6. Validação das Autoridades

3.2.7. Critérios para interoperação

### **3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES**

3.3.1. Identificação e autenticação para rotina de novas chaves

3.3.2. Identificação e autenticação para novas chaves após a revogação

### **3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO**

## **4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO**

Os itens seguintes estão referidos nos correspondentes itens da DPC AC CNDL RFB.

### **4.1. SOLICITAÇÃO DE CERTIFICADO**

4.1.1. Quem pode submeter uma solicitação de certificado

4.1.2. Processo de registro e responsabilidades

### **4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO**

4.2.1. Execução das funções de identificação e autenticação

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.3. Tempo para processar a solicitação de certificado

### **4.3. EMISSÃO DE CERTIFICADO**

4.3.1. Ações da AC durante a emissão de um certificado

4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

### **4.4. ACEITAÇÃO DE CERTIFICADO**

4.4.1. Conduta sobre a aceitação do certificado

4.4.2. Publicação do certificado pela AC

4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades

### **4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO**

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

### **4.6. RENOVAÇÃO DE CERTIFICADOS**

4.6.1. Circunstâncias para renovação de certificados

4.6.2. Quem pode solicitar a renovação

4.6.3. Processamento de requisição para renovação de certificados

4.6.4. Notificação para nova emissão de certificado para o titular

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6. Publicação de uma renovação de um certificado pela AC

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

#### **4.7 NOVA CHAVE DE CERTIFICADO**

4.7.1. Circunstâncias para nova chave de certificado

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

4.7.3. Processamento de requisição de novas chaves de certificado

4.7.4. Notificação de emissão de novo certificado para o titular

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

4.7.6. Publicação de uma nova chave certificada pela AC

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

#### **4.8. MODIFICAÇÃO DE CERTIFICADO**

4.8.1. Circunstâncias para modificação de certificado

4.8.2. Quem pode requisitar a modificação de certificado

4.8.3. Processamento de requisição de modificação de certificado

4.8.4. Notificação de emissão de novo certificado para o titular

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

4.8.6. Publicação de uma modificação de certificado pela AC

4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades

#### **4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO**

4.9.1. Circunstâncias para revogação

4.9.2. Quem pode solicitar revogação

4.9.3. Procedimento para solicitação de revogação

4.9.4. Prazo para solicitação de revogação

4.9.5. Circunstâncias para suspensão

4.9.6. Quem pode solicitar suspensão

4.9.7. Procedimento para solicitação de suspensão

4.9.8. Limites no período de suspensão

4.9.9. Frequência de emissão de LCR

4.9.10. Latência máxima para a LCR

4.9.11. Disponibilidade para revogação ou verificação de status on-line

- 4.9.12. Requisitos para verificação de revogação on-line
- 4.9.13. Outras formas disponíveis para divulgação de revogação
- 4.9.14. Tempo em que a AC deve processar o pedido de revogação
- 4.9.15. Requisitos especiais para o caso de comprometimento de chave
- 4.9.16. Requisitos de verificação de revogação para as partes confiáveis

#### **4.10. SERVIÇOS DE STATUS DE CERTIFICADO**

- 4.10.1. Características operacionais
- 4.10.2. Disponibilidade dos serviços
- 4.10.3. Funcionalidades operacionais

#### **4.11. ENCERRAMENTO DE ATIVIDADES**

#### **4.12. CUSTÓDIA E RECUPERAÇÃO DE CHAVE**

- 4.12.1. Política e práticas de custódia e recuperação de chave
- 4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

### **5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES**

Os itens seguintes estão referidos nos correspondentes itens da DPC AC CNDL RFB.

#### **5.1. CONTROLES FÍSICOS**

- 5.1.1. Construção e localização das instalações
- 5.1.2. Acesso físico
- 5.1.3. Energia e ar condicionado
- 5.1.4. Exposição à água
- 5.1.5. Prevenção e proteção contra incêndio
- 5.1.6. Armazenamento de mídia
- 5.1.7. Destruição de lixo
- 5.1.8. Instalações de segurança (backup) externas (off-site)

#### **5.2. CONTROLES PROCEDIMENTAIS**

- 5.2.1. Perfis qualificados
- 5.2.2. Número de pessoas necessário por tarefa
- 5.2.3. Identificação e autenticação para cada perfil
- 5.2.4. Funções que requerem separação de deveres

**5.3. CONTROLES DE PESSOAL**

- 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade
- 5.3.2. Procedimentos de verificação de antecedentes
- 5.3.3. Requisitos de treinamento
- 5.3.4. Frequência e requisitos para reciclagem técnica
- 5.3.5. Frequência e sequência de rodízio de cargos
- 5.3.6. Sanções para ações não autorizadas
- 5.3.7. Requisitos para contratação de pessoal
- 5.3.8. Documentação fornecida ao pessoal

**5.4. PROCEDIMENTOS DE LOG DE AUDITORIA**

- 5.4.1. Tipos de eventos registrados
- 5.4.2. Frequência de auditoria de registros (logs)
- 5.4.3. Período de retenção para registros (logs) de auditoria
- 5.4.4. Proteção de registro (log) de auditoria
- 5.4.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria
- 5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)
- 5.4.7. Notificação de agentes causadores de eventos
- 5.4.8. Avaliações de vulnerabilidade

**5.5. ARQUIVAMENTO DE REGISTROS**

- 5.5.1. Tipos de registros arquivados
- 5.5.2. Período de retenção para arquivo
- 5.5.3. Proteção de arquivo
- 5.5.4. Procedimentos para cópia de segurança (backup) de arquivo
- 5.5.5. Requisitos para datação de registros
- 5.5.6. Sistema de coleta de dados de arquivo (interno e externo)
- 5.5.7. Procedimentos para obter e verificar informação de arquivo

**5.6. TROCA DE CHAVE****5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE**

- 5.7.1. Recursos computacionais, software ou dados são corrompidos
- 5.7.2. Procedimentos no caso de comprometimento de chave privada de entidade

**5.7.3.** Capacidade de continuidade de negócio após desastre

## **5.8. EXTINÇÃO DE AC**

## **6. CONTROLES TÉCNICOS DE SEGURANÇA**

Nos itens seguintes são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC da AC CNDL RFB. São também definidos outros controles técnicos de segurança utilizados pela AC e pelas AR vinculadas na execução de suas funções operacionais.

### **6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES**

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [3].

#### **6.1.1. GERAÇÃO DO PAR DE CHAVES**

**6.1.1.1.** Quando o titular de certificado é uma pessoa física, esta é a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado é uma pessoa jurídica, esta indica por seu (s) representante (s) legal (is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

**6.1.1.1.1.** Item não aplicável.

**6.1.1.1.2.** Item não aplicável.

**6.1.1.2.** O processo de geração de chaves do tipo A1, contemplado nesta PC, exige:

- a) A instalação de software relacionado ao repositório armazenador do certificado selecionado pelo cliente;
- b) O par de chaves será gerado em repositório protegido por senha e/ou identificação biométrica e cifrado por software;
- c) O responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

**6.1.1.3.** O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

**6.1.1.4.** Após ser gerada, a chave privada da entidade titular, é gravada cifrada por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3], em repositório protegido por senha e/ou identificação biométrica, cifrado por software.

**6.1.1.5.** A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e o repositório utilizado para o seu armazenamento.

**6.1.1.6.** O processo de geração do par de chaves assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada é única e seu sigilo é suficientemente assegurado;
- b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

**6.1.1.7.** O repositório de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

**6.1.1.8.** Item não aplicável.

#### **6.1.2. ENTREGA DA CHAVE PRIVADA À ENTIDADE**

Item não aplicável.

#### **6.1.3. ENTREGA DA CHAVE PÚBLICA PARA O EMISSOR DE CERTIFICADO**

A entidade titular do certificado, através de seu software de acionamento, entrega sua chave pública à AC CNDL RFB ou a correspondente AR vinculada, por meio eletrônico, em formato PKCS#10.

#### **6.1.4. ENTREGA DA CHAVE PÚBLICA DA AC CNDL RFB AS TERCEIRAS PARTES**

A AC CNDL RFB disponibiliza o seu certificado, e de todos os certificados da cadeia V2 e v5 de certificação, para os usuários da ICP-Brasil, através:

a) No momento da disponibilização de um certificado para seu titular; usando formato PKCS#7 conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [3].

b) Diretório;

c) Página Web da AC CNDL RFB: <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil

e) Repositório da ICP-Brasil.

#### **6.1.5. TAMANHOS DE CHAVE**

**6.1.5.1.** Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira V2 e V5 o tamanho mínimo admitido para chaves criptográficas é de 2048 bits.

**6.1.5.2.** Os algoritmos e os tamanhos de chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

#### **6.1.6. GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS**

Os parâmetros de geração e verificação de chaves assimétricas das entidades titulares de certificados adotarão o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [3].

#### **6.1.7. PROPÓSITOS DE USO DE CHAVE (CONFORME O CAMPO “KEY USAGE” NA X.509 V3)**

Os pares de chaves correspondentes aos certificados emitidos pela AC CNDL RFB podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para



a garantia do não repúdio e para cifragem de chaves. Para isso, os certificados emitidos segundo esta PC têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

## **6.2. PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO**

O repositório de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada é única e seu sigilo é suficientemente assegurado;
- b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros através de recursos nativos do próprio sistema operacional. Também podem ser utilizados recursos adicionais de proteção como a definição de senhas para utilização e exportação da chave privada. Fica a critério do titular a configuração e utilização destes recursos adicionais de proteção.

### **6.2.1. PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO**

Item não aplicável.

### **6.2.2. CONTROLE DE “N DE M” PARA CHAVE PRIVADA**

Item não aplicável.

### **6.2.3. CUSTÓDIA (ESCROW) DE CHAVE PRIVADA**

A AC CNDL não realiza a custódia (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

### **6.2.4. CÓPIA DE SEGURANÇA (BACKUP) DE CHAVE PRIVADA**

**6.2.4.1.** Como diretriz geral, qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

**6.2.4.2.** A AC CNDL RFB não mantém cópia de segurança de chave privada de titular de certificado por ela emitido.

**6.2.4.3.** Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL, e protegida com um nível de segurança não inferior àquele definido para a chave principal.

**6.2.4.4.** Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realizar a geração de cópia de segurança da chave privada.

### **6.2.5. ARQUIVAMENTO DA CHAVE PRIVADA**

**6.2.5.1.** As chaves privadas das entidades titulares de certificados emitidos pela AC CNDL RFB não são arquivadas.

**6.2.5.2.** Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

#### **6.2.6. INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO**

Os Titulares de Certificados poderão optar por utilizar um hardware criptográfico, cartão inteligente ou token, para armazenar sua chave privada após a aceitação do certificado.

#### **6.2.7. ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO**

Ver item 6.1

#### **6.2.8. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA**

A chave privada é ativada, mediante senha solicitada pelo software de proteção da chave privada. A senha deve ser criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo. O Titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 03(três)meses.

#### **6.2.9. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA**

A desativação da chave privada ocorre em função da expiração do certificado correspondente ou em função de sua revogação.

#### **6.2.10. MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA**

Para destruição da chave privada de certificados emitidos conforme esta PC, é preciso que o usuário acesse o repositório de certificados do sistema operacional onde o certificado está instalado, localize o certificado e o remova do repositório. Este procedimento deve ser repetido em todos os locais onde o certificado foi instalado. Além disso é necessário apagar todas as cópias de segurança do certificado que porventura foram realizadas. A destruição da chave privada é irreversível e definitiva, não sendo mais possível a sua recuperação.

### **6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES**

#### **6.3.1. ARQUIVAMENTO DE CHAVE PÚBLICA**

As chaves públicas da AC CNDL RFB, dos titulares de certificados de assinatura digital e as LCR'S por ela emitidas permanecem armazenadas após a expiração dos certificados correspondentes permanentemente para verificação de assinaturas geradas durante seu período de validade.

#### **6.3.2. PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICAS E PRIVADAS**

**6.3.2.1.** As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

**6.3.2.2.** Item não aplicável.

**6.3.2.3.** O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC A1 da AC CNDL RFB A1 é de (um) ano.

**6.3.2.4.** Não se aplica.

**6.3.2.5.** Não se aplica.

## **6.4. DADOS DE ATIVAÇÃO**

### **6.4.1. GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO**

Os certificados de tipo A1 se utilizam, do repositório de certificados do sistema operacional para armazenamento de suas chaves privadas. Estes repositórios protegem as chaves privadas através de recursos nativos do próprio sistema operacional e não necessitam de dados de ativação para sua operação.

### **6.4.2. PROTEÇÃO DOS DADOS E ATIVAÇÃO**

Conforme descrito no item 6.4.1, os certificados emitidos conforme esta PC, não necessitam de dados de ativação para sua operação. Porém para uma maior proteção os titulares podem utilizar recursos adicionais como a definição de senhas para exportação das chaves privadas.

No caso de ativação por senha, recomenda-se:

- a) Nunca fornecer senha a terceiros;
- b) Escolher senhas de 8 (oito) ou mais caracteres; e
- c) Definir senhas com caracteres numéricos e alfanuméricos
- d) Memorizar a senha e
- e) Não a escrever

### **6.4.3. OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO**

Item não aplicável

## **6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL**

### **6.5.1. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL**

Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC CNDL RFB, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

- a) Senha de BIOS ativada;
- b) Controle de acesso lógico ao sistema operacional;
- c) Exigência de uso de senhas fortes;
- d) Diretivas de senha e de bloqueio de conta;
- e) Antivírus, antitrojan e antispysware, instalados, atualizados e habilitados;
- f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
- h) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio.

**6.5.2. CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL**

Item não aplicável.

**6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA****6.6.1. CONTROLES DE DESENVOLVIMENTO DE SISTEMA**

Item não aplicável.

**6.6.2. CONTROLES DE GERENCIAMENTO DE SEGURANÇA**

Item não aplicável.

**6.6.3. CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA**

Item não aplicável.

**6.6.4. CONTROLES NA GERAÇÃO DE LCR**

Antes de publicadas, todas as LCRs geradas pela AC CNDL RFB são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

**6.7. CONTROLES DE SEGURANÇA DE REDE**

Item não aplicável.

**6.8. CARIMBO DO TEMPO**

Item não aplicável.

**7. PERFIS DE CERTIFICADO, LCR**

Os itens seguintes especificam os formatos dos certificados e das LCRs gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

**7.1. PERFIL DO CERTIFICADO**

Os certificados emitidos pela AC CNDL RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

**7.1.1. NÚMERO (S) DE VERSÃO**

Os certificados emitidos pela AC CNDL RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

**7.1.2. EXTENSÕES DE CERTIFICADO**

**7.1.2.1.** Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticidade.

**7.1.2.2.** A ICP-Brasil define como obrigatórias as seguintes extensões:

- a) "Authority Key Identifier", não crítica: o campo key Identifier contém o hash SHA-1 da chave pública da AC CNDL RFB;
- b) "Key Usage", crítica: configurados conforme disposto no item 7.1.2.7. deste documento;

c) "Certificate Policies", não crítica:

c.1) O campo PolicyIdentifier contém o OID desta PC: 2.16.76.1.2.1.52

c.2) O campo Policyqualifiers contém e o endereço Web da DPC AC CNDL RFB <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

d) "CRL Distribution Points", não crítica: contém o endereço na Web onde se obtém a LCR correspondente:

Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira v2:

d.1) <http://repositorio.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv2.crl>

d.2) <http://repositorio2.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv2.crl>

Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira v5:

d.3) <http://repositorio.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv5.crl>

d.4) <http://repositorio2.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv5.crl>

e) "Authority Information Access", não crítica: a primeira entrada contém o método de acesso *id-ad-calssuer*, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

Raiz v2:

e.1) <http://repositorio.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv2.crl>

Raiz v5:

e.2) <http://repositorio.acspcbrasil.org.br/ac-cndlrfb/lcr-ac-cndlrfbv5.crl>

### 7.1.2.3. SUBJECT ALTERNATIVE NAME

A ICP-Brasil define como obrigatória a extensão "Subject Alternative Name", não crítica, e com os seguintes formatos:

a) Para Certificados de Pessoa Física (e-CPF) A (1):

a1) 3 (três) campos otherName, obrigatórios, contendo, nesta ordem:

i. OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular do certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o número de inscrição no Cadastro de Pessoa Física (CPF) do titular do certificado; nas 11 (onze) posições subsequentes, o número de Identificação Social do titular do certificado - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular do certificado; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

ii. OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) do titular do certificado.

iii. OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor do titular do certificado; nas 3 (três) posições subsequentes, o número correspondente a Zona Eleitoral; nas 4 (quatro) posições seguintes, o número correspondente

a Seção; nas 22 (vinte e duas) posições subsequentes, o nome do município e a UF do Título de Eleitor.

a.2) campos *otherName*, não obrigatórios, contendo:

I) OID = 2.16.76.1.4.n e conteúdo = de tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

A AC Raiz, por meio do documento ATRIBUIÇÃO DE OID NA ICPBRASIL [2] regulamentará a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.

II) OID = 1.3.6.1.4.1.311.20.2.3 com o seguinte conteúdo: este campo *Principal Name* contém a Identificação do endereço de login do titular do certificado no diretório Active Direct (AD) Microsoft.

a.3) Item não aplicável.

a.4) Item não aplicável.

**Nota:** No que se refere à pessoa física titular do certificado, o preenchimento dos campos abaixo, é obrigatório:

- Nome;
- Número de inscrição no CPF;
- Data de nascimento;
- E-mail.

b) para Certificados de Pessoa Jurídica (e-CNPJ) A (1):

b.1) 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

i. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o número de inscrição no Cadastro de Pessoa Física (CPF) do responsável pela Pessoa Jurídica perante o CNPJ; nas 11 (onze) posições subsequentes, o Número de Inscrição Social - NIS (PIS, PASEP ou CI) do responsável pela Pessoa Jurídica perante o CNPJ; nas 15 (quinze) posições subsequentes, o número do RG do responsável pela Pessoa Jurídica perante o CNPJ; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica, perante o CNPJ.

iii. OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

iv. OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da Pessoa Jurídica titular do certificado.

O preenchimento dos campos abaixo é obrigatório:

Da empresa:

- Número de inscrição no CNPJ da Pessoa Jurídica titular do certificado;
- Nome empresarial da pessoa jurídica titular do certificado;

Do responsável pela pessoa Jurídica perante o CNPJ:

- Nome do responsável pela Pessoa Jurídica perante o CNPJ;
- Número de inscrição no CPF do responsável pela Pessoa Jurídica perante o CNPJ;
- Data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ;
- E-mail do responsável pela Pessoa Jurídica perante o CNPJ.

c) Item não aplicável

d) Item não aplicável

e) Item não aplicável

**7.1.2.4.** Os campos `otherName` definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo `otherName` deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

b) Quando os números de NIS (PIS, PASEP ou CI), RG, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher o campo de órgão emissor. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas informações de tamanho variável referentes a números, tais como RG ou Título de Eleitor, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z e de 0 a 9, observado disposto no item 7.1.5.2 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

h) Item não aplicável.

**NOTA 01:** Para o preenchimento do campo Principal Name serão permitidos os caracteres de "A" a "Z", de "0" a "9" além dos caracteres "." (ponto), "-" (hífen) e "@" (arroba), necessários à formação do endereço de e-mail do responsável pelo uso do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

**Nota 2:** O campo `rfc822Name`, parte da extensão obrigatória "Subject Alternative Name", contendo o endereço e-mail do titular do certificado também deverá estar presente.

**7.1.2.5.** Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC CNDL RFB, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

**7.1.2.6.** Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

**7.1.2.7.** As extensões "*Key Usage*" e "*Extended Key Usage*" para os referidos tipos de certificado são obrigatórias e obedecem aos propósitos de uso e a criticalidade conforme descrição abaixo:

- a) Não se aplica
- b) Não se aplica
- c) Não se aplica
- d) Não se aplica
- e) Não se aplica
- f) para os demais certificados de Assinatura e/ou Proteção de e-Mail:

**"Key Usage"**, crítica: somente os seguintes *bits* devem estar ativados:

- *digitalSignature*;
- *nonRepudiation*; e
- *keyEncipherment*

**"Extended Key Usage"**, não crítica: deve conter os seguintes valores representados por seus respectivos OID:

- "**client authentication**", obrigatória: OID = 1.3.6.1.5.5.7.3.2, para autenticação de cliente;
- "**e-mail protection**", obrigatória: OID = 1.3.6.1.5.5.7.3.4, para proteção de e-mail;
- "**smartcard logon**", opcional: OID = 1.3.6.1.4.1.311.20.2.2, para login em estações de trabalho (UPN).
- Podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PC, em conformidade com a RFC 5280.

- g) Não se aplica

### **7.1.3. IDENTIFICADORES DE ALGORITMO**

Os certificados emitidos pela AC CNDL RFB às entidades titulares de certificado são assinados com o uso do algoritmo RSA SHA-256 como função de hash (OID 1.2.840.113549.1.1.11) conforme o padrão PKCS#1.



#### 7.1.4. FORMATOS DE NOME

##### 7.1.4.1. Certificado e-CPF

O nome do titular do certificado, constante do campo “Subject”, adota o “Distinguished Name” (DN) do padrão ITU X.500/ISO 9594:

a) Para Certificados e-CPF emitidos pela AC CNDL RFB v2 e v5:

- CN= Nome da Pessoa Física: número de inscrição no CPF
- OU = <Tipo de identificação utilizada>
- OU= CNPJ da AR onde ocorreu a identificação presencial> ou <CNPJ da AR que operou videoconferência> ou <Renovação Eletrônica>
- OU= Domínio do certificado (Opcional)
- OU= RFB e-CPF A1
- OU= Secretaria da Receita Federal do Brasil – RFB
- O= ICP-Brasil
- C= BR

Onde:

O Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com cumprimento máximo de 52 (cinquenta e dois) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.

São cinco os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:

- a) Primeiro “OU” Informando o tipo de identificação utilizada (presencial, videoconferência ou certificado digital);
- b) Segundo “OU” informando o CNPJ da AR onde ocorreu a identificação presencial; ou CNPJ da AR cujo AGR operou videoconferência para emissão do certificado; ou, ainda, a expressão “Renovação Eletrônica”, para os casos de renovação online com certificado digital válido;
- c) Terceiro “OU” com conteúdo variável, informando no campo domínio a identificação da empresa ou órgão fornecedor do certificado, quando o titular for seu empregado, funcionário ou servidor. Caso esse “OU” não seja utilizado, o mesmo deverá ser grafado com o texto “EM BRANCO”;
- d) Quarto “OU” com conteúdo fixo “RFB e-CPF A1”;
- e) Quinto “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo *Country Name* (C) com conteúdo fixo igual a “BR”.

O campo *Organization Name* (O) com conteúdo fixo igual a “ICP-Brasil”.

##### Certificado e-CNPJ:

a) Para Certificados emitidos pela AC CNDL RFB v2 e v5:

- CN= Nome Empresarial: número de inscrição no CNPJ
- OU = <Tipo de identificação utilizada>
- OU= RFB e-CNPJ A1
- OU= Secretaria da Receita Federal do Brasil – RFB
- OU= <CNPJ da AR onde ocorreu a identificação presencial> ou <CNPJ da AR que operou videoconferência> ou <Renovação Eletrônica>
- L = cidade
- ST= sigla da unidade da federação

O=ICP-Brasil

C=BR

Onde:

O *Common Name* (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com cumprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

O campo *locality* (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.

São quatro os campos *Organizational Unit* (OU) definidos no certificado, sendo assim constituídos:

- a) Primeiro "OU" informando o tipo de identificação utilizada (presencial, videoconferência ou certificado digital);
- b) Segundo "OU" com conteúdo fixo "RFB e-CNPJ A1";
- c) Terceiro "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil – RFB"
- d) Quarto "OU" informando o CNPJ da AR onde ocorreu a identificação presencial; ou CNPJ da AR cujo AGR operou videoconferência para emissão do certificado; ou, ainda, a expressão "Renovação Eletrônica", para os casos de renovação online com certificado digital válido.

O campo *Country Name* (C) com conteúdo fixo igual a "BR".

O campo *Organization Name* (O) com conteúdo fixo igual a "ICP-Brasil".

O campo *state or province name* (ST) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

**Nota:** No formato, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

**7.1.4.2.** Item não aplicável.

**7.1.4.3.** Item não aplicável.

**7.1.4.4.** Item não aplicável.

Nota: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

### **7.1.5. RESTRIÇÕES DE NOME**

**7.1.5.1.** Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

**7.1.5.2.** As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC CNDL RFB são as seguintes:

- a) Os acentos, tremas ou cedilhas não devem ser utilizados e devem ser substituídos pelo caractere não acentuado;
- b) Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
Branco	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
\$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(	28	?	3F
)	29	@	40
*	2A	\	5C

#### 7.1.6. OID (Object Identifier) da PC

O OID (Object Identifier) desta PC é 2.16.76.1.2.1.52

#### 7.1.7. USO DA EXTENSÃO "Policy Constraints"

Item não aplicável.

#### 7.1.8. SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nos certificados emitidos segundo esta PC, o campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC-AC CNDL RFB <http://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

#### 7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

### 7.2. PERFIL DE LCR

#### 7.2.1. NÚMERO (S) DE VERSÃO

As LCRs geradas pela AC CNDL RFB implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

#### 7.2.2. EXTENSÕES DE LCR E DE SUAS ENTRADAS

**7.2.2.1.** Neste item são descritas todas as extensões de LCR utilizadas pela AC CNDL RFB e sua criticidade.

**7.2.2.2.** As LCR'S da AC CNDL RFB obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

**7.2.2.2.1. Para LCR'S emitidos pela AC CNDL RFB**

- a) "Authority Key Identifier" não crítica: contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC CNDL RFB;

**7.3. PERFIL DE OCSP****7.3.1. NÚMERO DE VERSÃO**

Item não aplicável.

**7.3.2. EXTENSÕES DE OCSP**

Item não aplicável.

**8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES**

Os itens seguintes estão referidos em seus correspondentes na DPC AC CNDL RFB.

**8.1. FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES****8.2. IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR****8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA****8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO****8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA****8.6. COMUNICAÇÃO DOS RESULTADOS****9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS**

Os itens seguintes estão referidos em seus correspondentes na DPC AC CNDL RFB.

- 9.1. TARIFAS
  - 9.1.1. TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS
  - 9.1.2. TARIFAS DE ACESSO AO CERTIFICADO
  - 9.1.3. TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS
  - 9.1.4. TARIFAS PARA OUTROS SERVIÇOS
  - 9.1.5. POLÍTICA DE REEMBOLSO
- 9.2. RESPONSABILIDADE FINANCEIRA
  - 9.2.1. COBERTURA DE SEGURO
  - 9.2.2. OUTROS ATIVOS
  - 9.2.3. COBERTURA DE SEGUROS OU GARANTIA PARA ENTIDADES FINAIS
- 9.3. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO
  - 9.3.1. ESCOPO DE INFORMAÇÕES CONFIDENCIAIS
  - 9.3.2. INFORMAÇÕES FORA DO ESCOPO DE INFORMAÇÕES CONFIDENCIAIS
  - 9.3.3. RESPONSABILIDADE EM PROTEGER A INFORMAÇÃO CONFIDENCIAL
- 9.4. PRIVACIDADE DA INFORMAÇÃO PESSOAL
  - 9.4.1. PLANO DE PRIVACIDADE
  - 9.4.2. TRATAMENTO DE INFORMAÇÃO COMO PRIVADAS
  - 9.4.3. INFORMAÇÕES NÃO CONSIDERADAS PRIVADAS
  - 9.4.4. RESPONSABILIDADE PARA PROTEGER A INFORMAÇÃO PRIVADA
  - 9.4.5. AVISO E CONSENTIMENTO PARA USAR INFORMAÇÕES PRIVADAS
  - 9.4.6. DIVULGAÇÃO EM PROCESSO JUDICIAL OU ADMINISTRATIVO
  - 9.4.7. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO
- 9.5. DIREITO DE PROPRIEDADE INTELECTUAL

**9.6. DECLARAÇÕES E GARANTIAS****9.6.1. DECLARAÇÕES E GARANTIAS DA AC****9.6.2. DECLARAÇÕES E GARANTIAS DA AR****9.6.3. DECLARAÇÕES E GARANTIAS DO TITULAR****9.6.4. DECLARAÇÕES E GARANTIAS DAS TERCEIRAS PARTES****9.6.5. REPRESENTAÇÕES E GARANTIAS DE OUTROS PARTICIPANTES****9.7. ISENÇÃO DE GARANTIAS****9.8. LIMITAÇÕES DE RESPONSABILIDADES****9.9. INDENIZAÇÕES****9.10. PRAZO E RESCISÃO****9.10.1. PRAZO****9.10.2. TÉRMINO****9.10.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA****9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES****9.12. ALTERAÇÕES****9.12.1. PROCEDIMENTO PARA EMENDAS**

Alterações nesta PC são definidas pelo setor de Compliance da AC CNDL RFB. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.

**9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS**

A AC CNDL RFB mantém a versão corrente desta PC para consulta pública em seu repositório Web, no endereço: <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>

**9.12.3. CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO****9.13. SOLUÇÃO DE CONFLITOS****9.14. LEI APLICÁVEL****9.15. CONFORMIDADE COM A LEI APLICÁVEL****9.16. DISPOSIÇÕES DIVERSAS****9.16.1. ACORDO COMPLETO**

Esta PC representa as obrigações e deveres aplicáveis à AC CNDL RFB e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

**9.16.2. CESSÃO****9.16.3. INDEPENDÊNCIA DE DISPOSIÇÕES****9.16.4. EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)****9.17. OUTRAS PROVISÕES**

Esta PC foi submetida à aprovação, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC CNDL RFB.

**10. DOCUMENTOS REFIRENCIADOS****10.1. RESOLUÇÕES DO COMITÊ-GESTOR DA ICP BRASIL**

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.it.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA ICP-BRASIL	DOC-ICP-17
[6]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04

**10.2. INSTRUÇÕES NORMATIVAS DA AC RAIZ**

Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio

<http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

<b>Ref.</b>	<b>Nome do documento</b>	<b>Código</b>
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	DOC-ICP-04.01