Política de Certificado A1 da Autoridade Certificadora DOCCLOUD RFB [PC A1 da AC DOCCLOUD RFB]

[OID: 2.16.76.1.2.1.58]
Versão 6.0 de 05.08.2020

CONTROLE DE ALTERAÇÕES

RESPONSÁVEL	APROVAÇÃO	DESCRIÇÃO DA ALTEAÇÃO	VERSÃO	DATA
Compliance	Versão Inicial		1.0	12.06.2015
Compliance	Resolução 116 - 2015	Referência à autoridade certificadora Raiz V5 e suas cadeias subsequentes	2.0	29.08.2018
Compliance	Resolução 118 - 2015	Aprova a retirada do campo AIA da LCR e define a obrigatoriedade de dois pontos de obtenção da LCR em novas cadeias de certificação digital ICP-Brasil	2.0	29.08.2018
Compliance	IN nº 07 - 2016	conformidade aos requisitos do programa de raízes confiáveis para manutenção dos certificados da AC RAIZ da ICP-Brasil nos repositórios dos navegadores de internet	2.0	29.08.2018
Compliance	Resolução 119 - 2017	Obrigatoriedade de realização de auditorias WebTrust.	2.0	29.08.2018
Compliance	Resolução 123 - 2017	Procedimentos de validação fora do ambiente físico da AR.	2.0	29.08.2018
Compliance		Atualização das Informações de contato da AC.	2.1	05.12.2018
Compliance	Resolução 150 - 2018	7.1.4	3.0	04.04.2019
Compliance	Resolução 151 e 154 - 2019	Atualização das informações conforme resoluções	4.0	21.10.2019
Compliance	Instruções Normativas 02 e 03 de 2020	Solicitação de Certificado Digital por videoconferência e Procedimentos para aprovação de normativos da AC.	5.0	07.05.2020

Compliance	Resolução 169	Adequação de Conteúdo	6.0	05.08.2020

CONTEÚDO

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. Esta "Política de Certificado" (PC) descreve as políticas de certificação de certificados de Assinatura Digital Tipo A1 da Autoridade Certificadora DOCCLOUD RFB – AC DOCCLOUD RFB para a Secretaria da Receita Federal do Brasil na Infraestrutura de Chaves Públicas Brasileira.

1.1.2 A estrutura desta PC está baseada no DOC-ICP-04 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [6].

1.1.3 O tipo de certificado emitido sob esta PC é o Tipo A1.

1.1.4 Item não aplicável.

1.1.5 Item não aplicável.

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 "Política de Certificado de assinatura digital Tipo A1 da Autoridade Certificadora DOCCLOUD para a Secretaria da Receita Federal do Brasil" e referida como "PC A1 da AC DOCCLOUD RFB". Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O **OID** (object identifier) desta PC é **2.16.76.1.2.1.58**.

1.2.2 Item não aplicável.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridades Certificadoras

1.3.1.1. Esta PC refere-se exclusivamente à AC DOCCLOUD RFB no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC DOCCLOUD RFB estão descritos na Declaração de Práticas de Certificação da AC DOCCLOUD RFB (DPC da AC DOCCLOUD RFB).

1.3.2. Autoridades de Registro

Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC DOCCLOUD RFB para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da https://www.acdoccloud.com.br/repositorio com a seguintes informações:

a) relação de todas as AR credenciadas;
b) relação de AR que tenham se descredenciado da cadeia da AC DOCCLOUD RFB, com respectiva data do descredenciamento.

1.3.3 Titulares do Certificado

Pessoas físicas ou jurídicas inscritas no CPF ou no CNPJ podem ser Titulares de Certificado e-CPF ou e-CNPJ Tipo A1, desde que não enquadradas na situação cadastral de CANCELADA ou NULA (pessoa física) ou na condição de BAIXADA, INAPTA, SUSPENSA ou NULA (pessoa jurídica), conforme o disposto nos incisos I e II do art. 6. da Instrução Normativa RFB n. 1077, de 29 de Outubro de 2010 e Anexo I da Portaria RFB / Sucor / Cotec nº 18, de 19 de fevereiro de 2019 (Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 4.4).

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

Os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviços de Confiança - PSC vinculados à AC DOCCLOUD RFB estão relacionados em sua página web www.acdoccloud.com.br

1.3.5.1 PSS, PSBios ou PSC são entidades utilizadas pela AC DOCCLOUD RFB ou pelas AR's vinculadas para desempenhar atividade descrita nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infraestrutura física e lógica;
b) disponibilização de recursos humanos especializados; ou
c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.4. USABILIDADE DO CERTIFICADO

1.4.1. Uso apropriado do certificado

1.4.1.1 Neste item são relacionadas as aplicações para as quais os certificados definidos nesta PC são adequados.

1.4.1.2 As aplicações e demais programas que admitem 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 A AC DOCCLOUD RFB leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos 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.

Os certificados emitidos pela AC DOCCLOUD 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.

1.4.1.4 Certificados de tipos A1 serão 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
Item não aplicável.

1.5. POLÍTICA DE ADMINISTRAÇÃO

Neste item estão incluídos nome, endereço e outras informações da AC DOCCLOUD RFB, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1. Organização administrativa do documento
AC DOCCLOUD RFB
DOCCLOUD SOLUCAO DIGITAL

1.5.2. Contatos
Endereço: Rua Gonçalves Dias, 519 – Jardim Girassol - Americana/SP - CEP: 13.465-670.
Telefone: (19) 3477-1144
Página Web: www.acdoccloud.com.br

1.5.3. Adequabilidade da DPC com PC's
AC DOCCLOUD RFB
Nome: Lucas Carvalho dos Santos
Departamento: NORMAS & COMPLIANCE

Telefone: (19) 3477-1144 / **E-mail:** complianceac@doccloud.com.br

1.5.4. Procedimentos de aprovação desta PC

Este documento foi analisado pela alta gestão da AC DOCCLOUD RFB e submetido ao Instituto de Tecnologia da Informação – ITI para aprovação. Os procedimentos de aprovação da PC da AC DOCCLOUD RFB são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNICOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF PKIX	Internet Engineering Task Force - Public-Key Infrastructured (X.509)
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
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	On-line 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	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSBIO	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestador de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SINRIC	Sistema Nacional de Registro de Identificação Civil
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 PUBLICAÇÕES E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

2.1. REPOSITÓRIOS

2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.4. CONTROLE DE ACESSO OS REPOSITÓRIOS

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

3.1. NOMEAÇÃO

3.1.1. Tipos de nomes
3.1.2. Necessidade de os nomes serem 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 DA IDENTIDADE

3.2.1. Método para comprovar a posse de chave privada
3.2.2. Autenticação da identificação da organização
3.2.3. Autenticação da identidade de equipamento ou aplicação

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

5.1.8. Instalações de segurança (backup) externas (off-site) para AC

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. CONTROLE 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
5.4.3. Período de retenção para registros de auditoria
5.4.4. Proteção de registros de auditoria
5.4.5. Procedimentos para cópia de segurança (Backup) de registros 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 de cópia 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. Procedimentos de gerenciamento de incidente e comprometimento
5.7.2. Recursos computacionais, software, e/ou dados corrompidos
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade
5.7.4. Capacidade de continuidade de negócio após desastre

5.8. EXTINÇÃO DA 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 A1 da AC DOCCLOUD RFB. São definidos também outros controles técnicos de segurança utilizados pela AC DOCCLOUD RFB e pelas ARs 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 ICP BRASIL [3].

6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará 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. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando CSP (Cryptographic Service Provider) existente na estação do solicitante apresentados pelo browser e, quando da geração, a chave privada é armazenada no HD da estação.

A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa – hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO - e protegida por senha de acesso.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A1.

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

6.1.1.6. A mídia de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. Esta mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC DOCCLOUD RFB e descrito nesta PC é o A1.

TIPO DE CERTIFICADO	MÍDIA ARMAZENADORA DE CHAVE CRIPTOGRÁFICA (Requisitos Mínimos)
A1	*Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.*

6.1.2. Entrega da chave privada à entidade titular
Item não aplicável.

6.1.3. Entrega da chave pública para o emissor de certificado
A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

6.1.4. Disponibilização de chave pública da AC para usuários
A AC DOCCLOUD RFB disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web:

http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv2.p7b (para cadeia V2) e
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv5.p7b (para cadeia V5).

6.1.5. Tamanhos de chave
6.1.5.1. Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz Brasileira (V2 e V5). O tamanho das chaves criptográficas associadas é de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A1 da ICP-Brasil está em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [1].

6.1.6 Geração de parâmetros de chaves assimétricas verificação da qualidade dos parâmetros
Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3)

Os certificados têm ativados os bits digitalSignature, nonRepudiation e keyEncipherment.

Os pares de chaves correspondentes aos certificados emitidos pela AC DOCCLOUD 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.

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

Nos itens seguintes, a PC define os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos pela AC DOCCLOUD RFB.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. Item não aplicável.

6.2.1.2. Os requisitos aplicáveis ao módulo criptográfico utilizado para geração de chaves criptográficas dos titulares de certificado seguem os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2. Controle “n de m” para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*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. Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC DOCCLOUD RFB responsável por esta PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1. A AC DOCCLOUD RFB não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

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
O titular de certificado de e-CPF ou e-CNPJ deve obrigatoriamente utilizar senha para a proteção de sua chave privada, de acordo com o art. 5. da Instrução Normativa RFB N.1077, de 29 de outubro de 2010.

6.2.9. Método de desativação de chave privada
O titular do certificado pode definir procedimentos necessários para a desativação de sua chave privada.

6.2.10. Método de destruição de chave privada
O titular do certificado pode definir procedimentos necessários para a destruição de sua chave privada.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública
As chaves públicas da AC DOCCLOUD RFB, de titulares dos certificados de assinatura digital e as LCRs emitidas pela AC DOCCLOUD RFB são armazenadas 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 pública e Privada
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 poderão ser utilizadas durante todo o período 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 Certificados do tipo A1 previstos nesta PC podem ter a validade de minutos, horas, dias e até **1 ano**.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC são descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

Para certificados de tipo A1, a geração e armazenamento do par de chaves são realizados em software, com capacidade de geração de chave, sendo ativado e protegido por senha, e/ou identificação biométrica.

6.4.2 Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

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

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção anti-vírus e criptografia 3DES para a chave privada, armazenada no HD.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

A AC DOCCLOUD RFB desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC DOCCLOUD RFB utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC DOCCLOUD RFB utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC DOCCLOUD RFB provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DOCCLOUD RFB.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A AC DOCCLOUD RFB verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas

através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC DOCCLOUD RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de segurança de ciclo de vida
Item não aplicável.

6.6.4 Controles na geração da LCR antes de publicadas
Antes de publicadas, todas as LCRs geradas pela AC DOCCLOUD 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 DE TEMPO

Item não aplicável.

7. PERFIS DE CERTIFICADO, LCR E OSCP

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.

7.1 PERFIL DO CERTIFICADO

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

7.1.1 Número de versão
Todos os certificados emitidos pela AC DOCCLOUD RFB, segundo esta PC, implementam a versão 3 de certificado definida no 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 certificados utilizadas e sua criticalidade.

7.1.2.2. A AC DOCCLOUD RFB implementa nos certificados emitidos segundo esta PC as seguintes extensões, definidas como obrigatórias pela ICP-Brasil:

a) "***Authority Key Identifier***", **não crítica**: contém o resumo SHA-1 da chave pública da AC DOCCLOUD RFB;

b) "***Key Usage***", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment são ativados;

c) "***Certificate Policies***", não crítica, contém

c.1) o campo *policyIdentifier* contém o OID desta PC ***2.16.76.1.2.1.58***;

c.2) o campo PolicyQualifiers contém o endereço *Web* onde se obtém a DPC da AC DOCCLOUD RFB, onde: http://repositorio.acdoccloud.com.br/ac-doccloudrfb/dpc-acdoccloudrfb.pdf

d) **"*CRL Distribution Points*", não crítica**: contém o endereço *URL* das páginas *Web* onde se obtém a LCR da AC DOCCLOUD RFB:

Para Certificados Digitais emitidos na cadeia V2:

d.1) http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl

d.2) http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl

d.3) http://acrepositorio.icpbrasil.gov.br/lcr/doccloud/lcr-ac-doccloudrfbv2.crl

Para Certificados Digitais emitidos da cadeia V5:

d.1) http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl

d.2) http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl

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

f1) **Para Certificados Digitais emitidos na cadeia V2:**
http://repositorio.acdoccloud.com.br/acdoccloudrfb/ac-doccloudrfbv2.p7b

f2) **Para Certificados Digitais emitidos na cadeia V5:**
http://repositorio.acdoccloud.com.br/acdoccloudrfb/ac-doccloudrfbv5.p7b

A segunda entrada pode conter o método de acesso **id-ad-ocsp**, com o respectivo endereço do respondedor OCSP, utilizando o protocolo de acesso HTTP, nos seguintes endereços, onde estas extensões somente serão aplicáveis para certificados de usuário final: http://ocsp.acdoccloud.com.br

7.1.2.3. A AC DOCCLOUD RFB e a ICP-Brasil também definem como obrigatória a extensão "Subject Alternative Name", não crítica, e com os seguintes formatos:

a) Para Certificados e-CPF

a.1) 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, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; 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 Específico do INSS (CEI) da pessoa física 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; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

iv. campo rfc822Name contendo o endereço e-mail do titular do certificado.

a.2) Item não aplicável.

a.3) Item não aplicável.

b) Para Certificados e-CNPJ

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 pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva unidade da federação.

ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado.

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:

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

7.1.2.4. Item não aplicável

7.1.2.5. Item não aplicável

7.1.2.6. A AC DOCCLOUD RFB implementa nos certificados emitidos segundo esta PC os seguintes campos, previstos na RFC 5280 e definidos como opcionais pela ICP-Brasil:

a) para Certificados de Pessoa Física (e-CPF)
a.1) extensão “Subject Alternative Name”:
i. sub-extensão "rfc822Name", contendo o endereço e-mail do titular do certificado. Esse campo é obrigatório em todos os certificados e-CPF.

ii. campo otherName com OID = 1.3.6.1.4.1.311.20.2.3 e conteúdo UPN (User Principal Name), com a identificação do endereço de login do titular do certificado no diretório ActiveDirect (AD) Microsoft. Esse campo é opcional, aplicável apenas em certificados e-CPF utilizados para logon de rede.

a.2) extensão "Extended Key Usage", não crítica, contendo o valor:

i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2). Esse campo é obrigatório em todos os certificados e-CPF;

ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4). Esse campo é obrigatório em todos os certificados e-CPF;

iii. “smart card logon” (id-ms-kp-smartcard-logon) (OID 1.3.6.1.4.1.311.20.2.2) Esse campo é opcional, aplicável apenas em certificados e-CPF utilizados para logon de rede.

b) para Certificados de Pessoa Jurídica (e-CNPJ)
b.1) extensão “Subject Alternative Name”
i. sub-extensão "rfc822Name", contendo o endereço e-mail do responsável, perante o CNPJ, pela Pessoa Jurídica titular do certificado. Esse campo é obrigatório em todos os certificados e-CNPJ.

b.2) extensão "Extended Key Usage", não crítica, contendo o valor:

i. "client authentication" (id-kp-clientAuth) (OID 1.3.6.1.5.5.7.3.2). Esse campo é obrigatório em todos os certificados e-CNPJ.

ii. "e-mail protection" (id-kp-emailProtection) (OID 1.3.6.1.5.5.7.3.4). Esse campo é obrigatório em todos os certificados e-CNPJ.

7.1.2.7. As extensões “Key Usage” e “Extended Key Usage” para os referidos tipos de certificado são obrigatórias e devem obedecer aos propósitos de uso e a criticalidade conforme descrição abaixo:

a) Para certificados de Assinatura de Resposta OCSP:

i. “Key Usage”, crítica: deve conter o bit digitalSignature ativado, podendo conter o bit nonRepudiation ativado;

ii. "Extended Key Usage", não crítica: somente o propósito OCSPSigning OID =1.3.6.1.5.5.7.3.9 deve estar presente;

b) Para os demais certificados de Assinatura e/ou Proteção de e-Mail:

i. “Key Usage”, crítica: deve conter o bit digitalSignature ativado, podendo conter os bits keyEncipherment e nonRepudiation ativados;

ii. “Extended Key Usage”, não crítica, contém no mínimo um dos propósitos “client authentication" (OID 1.3.6.1.5.5.7.3.2) e/ou "E-mail protection" (OID 1.3.6.1.5.5.7.3.4), e podendo conter o valor “Smart Card Logon” (OID 1.3.6.1.4.1.311.20.2.2), quando for utilizado o campo “UPN” na extensão “Subject Alternative Name”

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC DOCLOUD RFB são assinados utilizando o algoritmo RSA com 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

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

a) Para certificados e-CPF

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

Onde

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

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

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

- ✓ Primeiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”;
- ✓ Segundo “OU” Informando o CNPJ da AR onde ocorreu a identificação presencial, que será preenchido com 14 (quatorze) posições, sem caracteres como “.”, “/” ou “-“.
- ✓ Terceiro “OU” Informando tipo da validação ocorrida para emissão do Certificado Digital, sendo: presencial, videoconferência ou renovação online (Certificado Digital);
- ✓ Quarto “OU” com conteúdo fixo “RFB e-CPF A1”;
- ✓ Quinto “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”.

O Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com comprimento 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.

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

b) Para Certificados e-CNPJ
C = BR
O = ICP-Brasil
L = cidade
ST= <Sigla da unidade da federação>
OU = Secretaria da Receita Federal do Brasil – RFB
OU = CNPJ da AR onde ocorreu a identificação presencial
OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)
OU = RFB e-CNPJ A1
CN = Nome Empresarial: número de inscrição no CNPJ

Onde:

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

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

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

- ✓ Primeiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

- ✓ Segundo “OU” Informando o CNPJ da AR onde ocorreu a identificação presencial, que será preenchido com 14 (quatorze) posições, sem caracteres como “.”, “/” ou “-“.
- ✓ Terceiro “OU” Informando tipo da validação ocorrida para emissão do Certificado Digital, sendo: presencial, videoconferência ou renovação online (Certificado Digital);
- ✓ Quarto “OU” com conteúdo fixo “RFB e-CNPJ A1”;

O Common Name (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com comprimento 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.

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

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

7.1.5. Restrições de nome

7.1.5.1. Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC DOCCLOUD RFB são as seguintes:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

CARACTERE	CÓDIGO NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25

&	26
'	27
(	28
)	29
*	2ª
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (Object Identifier) de Política de Certificado
O OID atribuído a esta Política de Certificado é: ***2.16.76.1.2.1.58***.

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 da página *Web* (URL) com a DPC da AC DOCCLOUD RFB, sendo:
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/dpc-acdoccloudrfb.pdf

7.1.9. Semântica de processamento para extensões críticas
Extensões críticas são ser interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. Número de versão
As LCRs geradas pela AC DOCCLOUD RFB segundo a PC, implementam a versão 2 de LCR definida no 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 A AC DOCCLOUD RFB adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) **"*Authority Key Identifier*", não crítica:** contém o resumo SHA-1 da chave pública da AC DOCCLOUD RFB que assina a LCR; e

b) "***CRL Number*", não crítica**: contém número sequencial para cada LCR emitida pela AC que assina a LCR.

A AC DOCCLOUD RFB define como obrigatória a seguinte extensão para suas LCRs:

c) "***Authority Information Access***", não crítica: contém o endereço web onde se poderá obter a cadeia de certificação:

Para Certificados Digitais emitidos na cadeia V2:
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv2.p7b

Para Certificados Digitais emitidos na cadeia V5:
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv5.p7b

7.3. PERFIL DE OCSP

7.3.1. Número(s) de versão
Os serviços de respostas OCSP da AC DOCCLOUD RFB implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP
Os serviços de respostas OCSP da AC DOCCLOUD RFB estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

8.1. FREQUÊNCIA E CIRCUNSTÂNCIA DAS AVALIAÇÕES

8.2. IDENTIFICAÇÃO E 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 RESULTADO

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC DOCCLOUD 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 do 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 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 privadas
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. DIREITOS 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 RESPOSABILIDADE

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 podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC DOCCLOUD RFB. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos
A AC DOCCLOUD RFB mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web
http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloud-rfb-pc-a1.pdf

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 DOCCLOUD 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 da AC DOCCLOUD RFB foi submetida à aprovação, durante o processo de credenciamento da AC DOCCLOUD RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

10. DOCUMENTOS REFERENCIADOS

9.1. 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.iti.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 DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL*	DOC-ICP-17
[5]	*REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL*	DOC-ICP-12
[6]	*REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL*	DOC-ICP-04

9.2. 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.

REF.	*NOME DO DOCUMENTO*	*CÓDIGO*
[1]	*PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL*	*DOC-ICP-01.01*

[2]	*ATRIBUIÇÃO DE OID NA ICP-BRASIL*	*DOC-ICP-04.01*