Política de Certificado de Assinatura Tipo A3

PC A3 - AC CONSULTI BRASIL RFB

Versão 3.0

Maio 2020

AC CONSULTI BRASIL RFB

POLÍTICA DE CERTIFICADO DE ASSINATURA – TIPO A1

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou alteração	Item alterado
1.0	02/03/2016	N/A	-
2.0	24/10/2017	DOC-ICP-04	1.1, 1.3.4, 1.3.5, 6.1.4, 6.1.9, 6.2.4, 7.1.2.4, 7.1.2.6, 7.1.2.7, 7.1.2.8, 7.1.4.1, 7.1.4.2
		Resolução 116, de 2015	6.1.5, 7.1.2.2, 7.1.3
		Resolução 118, de 2015	7.1.2.2, 7.1.2.3
		Instrução Normativa n° 07, de 2016	
		DOC-ICP-05 e DOC-ICP-01.02	1.3.2.1, 1.3.3.1, 1.4, 6.1.4 “c”, 7.1.2.2.1, 7.1.2.2.1 “c.2”, 7.1.2.2.1 “d.2”, 7.1.2.2.2 “e”, 7.2.2.2 “c”, 8.2
2.1	01/04/2019	Resolução 119, de 2017	7.1.2.3 “a.4”
		Resolução 124, de 2017	7.1.2.8
		Resolução 132, de 2017	1.3.3A e 6.2.4.2
		Resolução 139, de 2018	6.1.1.1.2, 7.1.2.3
		Resolução 141, de 2018	7.1.2.3 “a”
		Resolução 150, de 2018 e Leiaute dos CDs da RFB, versão 4.4 de 02/2019	7.1.4.1
		DOC-ICP-04	1.3.5.4, 6.1.1.8, 6.1.2, 6.1.3, 6.1.5.1, 6.1.6, 6.1.9, 7.1.2.2.2, 7.1.2.5, 7.1.2.6, 7.1.4.2 “g” e “h”
		N/A	1.3.3.1, 1.4, 6.1.4 “c”, 8.2
3.0	24/04/2020	Resolução 151, de 30/05/2019 Aprova a versão 7.0 do DOC-ICP-04.	Diversos

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 Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1 VISÃO GERAL

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [5] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras (AC), integrantes da ICP-Brasil, na elaboração de suas Políticas de Certificado (PC).

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A3 da AC Consulti Brasil RFB, a seguir designada simplesmente por "PC A3 da AC Consulti Brasil RFB", adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [5].

1.1.3 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo A3.

1.1.4 Não se aplica.

1.1.5 Não se aplica.

1.1.6 Não se aplica.

1.1.7 Não se aplica.

1.1.8 Não se aplica.

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo A3 da Autoridade Certificadora Consulti Brasil RFB. O Object Identifier - OID da PC A3 da AC Consulti Brasil RFB, atribuído para esta

PC, na conclusão do processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.3.62**.

1.2.2 Não se aplica.

1.3 PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1 Esta PC se refere à AC Consulti Brasil RFB, integrante da 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 Consulti Brasil RFB estão descritos na Declaração de Práticas de Certificação da AC Consulti Brasil RFB (DPC - AC Consulti Brasil RFB).

1.3.2 AUTORIDADES DE REGISTRO

1.3.2.1 Os processos de recebimento, identificação 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). As ARs vinculadas à AC Consulti Brasil RFB estão relacionados na página https://acconsultibrasil.com.br/repositorio/ que contém:

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

1.3.3 TITULARES DO CERTIFICADO

Pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA ou NULA, e pessoas jurídicas inscritas no CNPJ, desde que não enquadradas na condição de INAPTA, SUSPENSA, BAIXADA ou NULA 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). Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB. Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

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

A relação de todos os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBios) e Prestadores de Serviço de Confiança (PSC), vinculados à AC Consulti Brasil RFB estão relacionados na página https://acconsultibrasil.com.br/repositorio/.

1.4 USABILIDADE DO CERTIFICADO

1.4.1 USO APROPRIADO DO CERTIFICADO

1.4.1.1 Os certificados definidos por esta PC têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação e 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 Consulti Brasil RFB leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos 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 tipos A3 emitidos pela AC Consulti Brasil RFB serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.
1.4.1.5 Não se aplica.
1.4.1.6 Não se aplica.
1.4.1.7 Não se aplica.
1.4.1.8 Não se aplica.

1.4.2 USO PROIBITIVO DO CERTIFICADO

Não se aplica.

1.5 POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Consulti Brasil RFB

1.5.2 CONTATOS

Endereço: Av. Castelo Branco, 4721 - Rodoviário, Goiânia - GO, 74430-130.

Telefone: +55 (62) 3933-0600

Página web: www.acconsultibrasil.com.br

E-mail: consultibrasil@consultibrasil.com.br

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Guilherme Franco Rodrigues

Telefone: +55 (62) 3933-0600

E-mail: guilherme@consultibrasil.com.br

Outros: Diretoria de Operações

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

Esta PC é aprovada pelo ITI. Os procedimentos de aprovação da PC da AC Consulti Brasil 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
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 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
ISSO	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 Consulti Brasil RFB.

2.1 Repositórios
2.2 Publicação de informações dos certificados
2.3 Tempo ou frequência de publicação
2.4 Controle de acesso aos repositórios

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Consulti Brasil 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 DE 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 um indivíduo
3.2.4 Informações não verificadas do titular do certificado
3.2.5 Validação das autoridades
3.2.6 Critérios para interoperação
3.2.7 Autenticação da Identidade de Equipamento ou Aplicação

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 em seus correspondentes na DPC - AC Consulti Brasil RFB.

4.1 SOLICITAÇÃO DO 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

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
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 Recursos computacionais, software, e/ou dados 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 DA AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

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 Não se aplica.

6.1.1.1.2 Não se aplica.

6.1.1.2 O processo de geração de chaves do tipo A3, contemplado nesta PC, exige:

a) A geração do par de chaves ocorre em cartão inteligente, token ou HSM com certificação INMETRO, protegidos por senha;
b) 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 [1].

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], em

hardware criptográfico e com certificação INMETRO.

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 pode eficazmente ser protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 A mídia 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 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos dos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇADA ICP-BRASIL [4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC Consulti Brasil RFB, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE

Item não aplicável.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA 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 ENTREGA DE CHAVE PÚBLICA DA AC CONSULTI BRASIL RFB ÀS TERCEIRAS PARTES

As formas para a disponibilização do certificado da AC Consulti Brasil RFB, e de todos os certificados da cadeia V2 e da cadeia V5 de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

a) No momento da disponibilização de um certificado para seu titular, usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1];
b) Diretório;
c) Página web:
d) Cad. v5: http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/ac-acconsultibrasilrfbv5.p7b
e) Cad. v5: http://repositorio2.acconsultibrasil.com.br/ac-acconsultibrasilrfb/ac-acconsultibrasilrfbv5.p7b
f) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil;
g) Repositório da ICP-Brasil.

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 Os certificados emitidos de acordo com esta PC situam-se sob as cadeias da Autoridade Certificadora Raiz V2 ou V5. O tamanho mínimo admitido para chaves criptográficas de titular final é de 2048 bits.

6.1.5.2 Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [1].

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

Os pares de chaves correspondentes aos certificados emitidos pela AC Consulti Brasil 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

A mídia 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, pois é gerada em cartão, token ou HSM com certificação INMETRO. Esses módulos criptográficos não permitem a exportação da chave privada e exigem senha para a sua utilização.

6.2.1 PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico utilizado na geração e utilização de chaves criptográficas possui certificação INMETRO.
6.2.1.2 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado seguem os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Não se aplica.

6.2.3 CUSTÓDIA (ESCROW) DE CHAVE PRIVADA

6.2.3.1 O agente de custódia (escrow) dos certificados emitidos pela AC Consulti Brasil RFB, é o PSC Consulti Brasil. As chaves privadas são armazenadas criptografadas em partições exclusivas em hardware criptográfico certificado pelo INMETRO. Estas chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e push notification).
6.2.3.2 A AC Consulti Brasil RFB não implementa a recuperação de chaves privadas.

6.2.4 CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

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

6.2.4.2 A AC Consulti Brasil RFB, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, no entanto em casos em que o CD é emitido utilizando o PSC Consulti Brasil, a guarda da cópia da chave privada é realizada pelo próprio PSC.
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 [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.
6.2.4.4 Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realizar a geração de cópia de segurança de sua chave privada.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 As chaves privadas das entidades titulares de certificados emitidos por esta PC 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

A AC Consulti Brasil RFB gera os pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

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 3 (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 software de proteção da chave privada, localize o certificado e o remova do repositório. 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 Consulti Brasil RFB, dos titulares de certificados de assinatura digital e as LCRs 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 Não se aplica.
6.3.2.3 O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC A3 da AC Consulti Brasil RFB é de 5 (cinco) anos.
6.3.2.4 Não se aplica.
6.3.2.5 Não se aplica.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC estão 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

Os certificados emitidos conforme esta PC, se utilizam de hardwares criptográficos para manter a segurança de suas chaves privadas. Estes hardwares possuem certificação INMETRO e protegem as

chaves privadas armazenando-as em partições exclusivas para este fim, com acesso restrito apenas através da utilização de senha criada pelo próprio titular, não necessitando de outros dados de ativação para sua operação. Em casos de emissão através de PSC, as chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e push notification).

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

Conforme descrito no item 6.4.1, os certificados emitidos conforme esta PC, não necessitam de outros dados de ativação para sua operação além da própria senha criada pelo titular e da posse do hardware criptográfico. Para uma maior proteção, os hardwares possuem a capacidade de bloquear o acesso à chave privada caso a quantidade de tentativas de utilização com a senha errada exceda o limite pré-definido. A AC Consulti Brasil RFB recomenda:

a) Nunca fornecer senha a terceiros;
b) Escolher senhas de 08 (oito) ou mais caracteres;
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

Não se aplica.

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 Consulti Brasil 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 antispyware*, 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 02 (dois) minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL

Não se aplica.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 CONTROLES DE DESENVOLVIMENTO DO SISTEMA

Como descrito no item correspondente da DPC AC Consulti Brasil RFB.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Como descrito no item correspondente da DPC AC Consulti Brasil RFB.

6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Como descrito no item correspondente da DPC AC Consulti Brasil RFB.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCRs geradas pela AC Consulti Brasil 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

Não se aplica.

6.8 CARIMBO DO TEMPO

Não se aplica.

7 PERFIS DE CERTIFICADO E LCR

Os itens seguintes especificam os formatos dos certificados e das LCRs geradas 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

Todos os certificados emitidos pela AC Consulti Brasil RFB, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 NÚMERO DE VERSÃO

Os certificados emitidos pela AC Consulti Brasil RFB, segundo esta PC, 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 criticalidade.

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

a) **"Authority Key Identifier"**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Consulti Brasil RFB;

b) **"Key Usage"**, crítica: configurados conforme disposto no item 7.1.2.7 deste documento;

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

c1) O campo PolicyIdentifier contém o OID desta PC: 2.16.76.1.2.1.51;

c2) O campo PolicyQualifiers contém o endereço Web onde se obtém a DPC AC Consulti Brasil RFB: http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/dpc-acconsultibrasilrfb.pdf.

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

Para certificados emitidos soba cadeia da Autoridade Certificadora Raiz Brasileira v5:

d1) http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/lcr-ac-acconsultibrasilrfbv4.crl

d2) http://repositorio2.acconsultibrasil.com.br/ac-acconsultibrasilrfb/lcr-acacconsultibrasilrfbv4.crl

e) **"Authority Information Access"**, não crítica: a primeira entrada contém o método de acesso

id-ad-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

e1) http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/ac-acconsultibrasilrfbv5.p7b

e2) http://repositorio2.acconsultibrasil.com.br/ac-acconsultibrasilrfb/ac-acconsultibrasilrfbv5.p7b

7.1.2.3 SUBJECT ALTERNATIVE NAME

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

a) Para Certificado de Pessoa Física:

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

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.

a2) campos otherName, não obrigatórios, contendo:

I). OID = 2.16.76.1.4.2.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.

NOTA: O preenchimento dos campos abaixo, referentes à pessoa física titular do certificado, é

obrigatório:

a) Nome;
b) Número de inscrição no CPF;
c) Data de nascimento;
d) E-mail.

a3) Não se aplica.

a4) Não se aplica.

b) Para Certificados de Pessoa Jurídica:

b1) 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 Registro Geral (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.

NOTA: Os seguintes campos são de preenchimento obrigatório:

Da empresa:

- Nome Empresarial;
- Número de inscrição no CNPJ.

Do responsável pela pessoa jurídica perante o CNPJ:

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

c) Não se aplica.
d) Não se aplica.
e) Não se aplica.

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 não estiver disponível, não se deve preencher o campo de órgão emissor e UF. 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, 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 o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;
h) Não se aplica.

Nota 1: 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 login do titular 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 Consulti Brasil 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 email;
- **"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 Consulti Brasil RFB às entidades titulares de certificado são assinados com o uso do 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

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

a) CERTIFICADO e-CPF

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

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, assim constituídos:

a) Primeiro "OU" Informando o CNPJ da AR onde ocorreu a identificação presencial;
b) Segundo "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil – RFB";
c) Terceiro "OU" com conteúdo fixo "RFB e-CPF A1";
d) Quarto "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 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.

b) CERTIFICADO e-CNPJ

CN = <Nome Empresarial>: <número de inscrição no CNPJ>
OU = RFB e-CNPJ A1
OU = Secretaria da Receita Federal do Brasil – RFB
OU = <CNPJ da AR onde ocorreu a identificação presencial>
L = <Cidade>

ST = <Sigla da unidade da federação>
O = ICP-Brasil
C = BR

Onde:
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.

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

a) Primeiro "OU" informando o CNPJ da AR onde ocorreu a identificação presencial;
b) Segundo "OU" com conteúdo fixo "RFB e-CNPJ A3";
c) Terceiro "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil – RFB".

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.

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 Não se aplica.
7.1.4.3 Não se aplica.
7.1.4.4 Não se aplica.
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 Consulti

Brasil 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)	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 **2.16.76.1.2.3.62.**

7.1.7 USO DA EXTENSÃO "*Policy Constraints*"

Não se aplica.

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 Consulti Brasil RFB: http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/dpc-acconsultibrasilrfb.pdf.

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 DE VERSÃO

As LCRs geradas pela AC Consulti Brasil 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 Consulti Brasil RFB e sua criticalidade.

7.2.2.2 As LCRs da AC Consulti Brasil RFB obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

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

b) **"CRL Number"**, não crítica: contém um número sequencial para cada LCR emitida pela AC Consulti Brasil RFB.

7.3 PERFIL DE OCSP

7.3.1 NÚMERO DE VERSÃO

Não se aplica.

7.3.2 EXTENSÕES DE OCSP

Não se aplica.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Consulti Brasil 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

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Consulti Brasil RFB.

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

A AC Consulti Brasil RFB segue um processo periódico de atualização de suas PCs, que contempla a revisão em duas etapas. A primeira realizada pela equipe de Compliance/ Segurança da Informação a segunda pela aprovação da Diretoria, visando a adequação dos documentos conforme as normas, procedimentos e regulamentos atuais da AC RFB e ICP-Brasil. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.

9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

A AC Consulti Brasil RFB mantém a versão corrente desta PC para consulta pública em seu

repositório web, no endereço: http://repositorio.acconsultibrasil.com.br/ac-acconsultibrasilrfb/ac-acconsultibrasil-rfb-pc-a3.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 Consulti Brasil 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 Consulti Brasil RFB.

10 DOCUMENTOS REFERENCIADOS

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 https://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 DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇADA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL	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 https://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