

Política de Certificado de Assinatura Tipo A1

PC A1 - AC SAFEWEB RFB

**Versão 5.0
Dezembro 2020**

SUMÁRIO

1	INTRODUÇÃO.....	5
1.1	VISÃO GERAL.....	5
1.2	NOME DO DOCUMENTO E IDENTIFICAÇÃO	5
1.3	PARTICIPANTES DA ICP-BRASIL.....	5
1.4	USABILIDADE DO CERTIFICADO	6
2	RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	9
2.1	Repositórios	9
2.2	Publicação de informações dos certificados.....	9
2.3	Tempo ou frequência de publicação.....	9
2.4	Controle de acesso aos repositórios.....	9
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	9
3.1	NOMEAÇÃO	9
3.2	VALIDAÇÃO INICIAL DE IDENTIDADE	9
3.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES.....	9
3.4	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	10
4	REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	10
4.1	SOLICITAÇÃO DO CERTIFICADO	10
4.2	PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	10
4.3	EMISSÃO DE CERTIFICADO	10
4.4	ACEITAÇÃO DE CERTIFICADO.....	10
4.5	USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO.....	10
4.6	RENOVAÇÃO DE CERTIFICADOS.....	10
4.7	NOVA CHAVE DE CERTIFICADO.....	11
4.8	MODIFICAÇÃO DE CERTIFICADO.....	11
4.9	SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	11
5	CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	12
5.1	CONTROLES FÍSICOS	12
5.2	CONTROLES PROCEDIMENTAIS	12
5.3	CONTROLES DE PESSOAL	12
6	CONTROLES TÉCNICOS DE SEGURANÇA	13
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES	13
6.2	PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO ...	16
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES	18
6.4	DADOS DE ATIVAÇÃO	18
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 E LCR.....	20
7.1	PERFIL DO CERTIFICADO	20
7.2	PERFIL DE LCR	28
7.3	PERFIL DE OCSP.....	28
8	AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	29
8.1	FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES	29
8.2	IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR.....	29

8.3	RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA.....	29
8.4	TÓPICOS COBERTOS PELA AVALIAÇÃO.....	29
8.5	AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	29
9	OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	29
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.....	30
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 REFERENCIADOS.....	31

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou alteração	Item alterado
1.0	15/12/2014	N/A	N/A
1.1	19/03/2015	N/A	7.1.2.2 "c.2", 7.1.2.2 "d.1" "d.2" "d.3", 7.1.2.2 "f", 7.1.8, 7.2.2.2 "c"
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 nº 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
4.0	15/07/2020	Resolução 169, de 17/04/2020. Aprova a versão 7.2 do DOC-ICP-04.	7.1.4.1
5.0	21/12/2020	Resolução CG ICP-Brasil nº 179, de 20/10/2020. Aprova a versão 8.0 do DOC-ICP-04.	1, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.1.11, 1.1.12, 1.3.3, 1.6, 6.1.1.3, 6.1.1.4, tabela 1, 6.1.4 "a", 6.1.5.2, 6.1.6, 6.2.4.3, 7.1.2.3 "a.2", 7.1.2.4 "c", 7.1.2.7 "f", 7.1.4 "a" e "b", 10.1, 10.2 e 11.

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] 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 A1 da AC Safeweb RFB, a seguir designada simplesmente por "PC A1 da AC Safeweb RFB" adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1].

1.1.3 A estrutura desta PC está baseada na RFC 3647.

1.1.4 Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.1.5 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo A1.

1.1.6 Os certificados A1 de assinatura estão associados aos requisitos menos rigorosos de segurança.

1.1.7 Os certificados A1 de assinatura podem ser emitidos para pessoas físicas ou jurídicas.

1.1.8 Não se aplica

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.1.11 Não se aplica.

1.1.12 Não se aplica.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo A1 da Autoridade Certificadora Safeweb RFB. O *Object Identifier* - OID da PC A1 da AC Safeweb RFB, atribuído para esta PC, na conclusão do processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.1.51**.

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 Safeweb RFB, integrante da ICP-Brasil, sob a hierarquia da Autoridade Certificadora Secretaria da Receita Federal do Brasil (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 Safeweb RFB estão descritos na

Declaração de Práticas de Certificação da AC Safeweb RFB (DPC - AC Safeweb 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 Safeweb RFB estão relacionados na página <https://safeweb.com.br/ac/autoridades-registro> 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 no Anexo I da Portaria RFB/Sucor/Cotec nº 42, de 07 de agosto de 2020 (Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 5.0). 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 Safeweb RFB estão relacionados na página <https://safeweb.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 Safeweb 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 A1 emitidos pela AC Safeweb 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 Safeweb RFB

1.5.2 CONTATOS

Endereço: Av. Princesa Isabel, 828, bairro Santana, Porto Alegre/RS, CEP 90620-000.

Telefone: +55 (51) 3018-0300

Página web: www.safeweb.com.br

E-mail: compliance@safeweb.com.br

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Gisele Strey

Telefone: + 55 (51) 3018-0300

E-mail: compliance@safeweb.com.br

Outros: Setor de Compliance

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

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

1.6 DEFINIÇÕES E ACRÔNIMOS

Tabela 1

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 ICP-Brasil	Comitê Gestor da ICP-Brasil
<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>
CNPJ	Cadastro Nacional de Pessoa Jurídica
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
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
PIS	Programa de Integração Social
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral

SAT	Sistema de Autenticação e Transmissão
SSL	Secure Socket Layer
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 Safeweb 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 Safeweb RFB.

3.1 NOMEAÇÃO

- 3.1.1 Tipos de nomes
- 3.1.2 Necessidade dos 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 Safeweb 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
- 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 Tempo em que a AC deve processar o pedido de revogação
- 4.9.6 Requisitos de verificação de revogação para as partes confiáveis
- 4.9.7 Frequência de emissão de LCR
- 4.9.8 Latência máxima para a LCR
- 4.9.9 Disponibilidade para revogação/verificação de status on-line
- 4.9.10 Requisitos para verificação de revogação on-line
- 4.9.11 Outras formas disponíveis para divulgação de revogação
- 4.9.12 Requisitos especiais para o caso de comprometimento de chave
- 4.9.13 Circunstâncias para suspensão
- 4.9.14 Quem pode solicitar suspensão
- 4.9.15 Procedimento para solicitação de suspensão
- 4.9.16 Limites no período de suspensão

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 em seus correspondentes na DPC - AC Safeweb RFB.

5.1 CONTROLES FÍSICOS

5.1.1 Construção e localização das instalações de AC

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) 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 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

- 5.7.2 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, 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 Safeweb 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 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 DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, em repositório protegido por senha e/ou identificação biométrica e cifrado por software, conforme a Tabela 2 a seguir.

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 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 Não se aplica.

Tabela 2 – Mídias Armazenadoras de Chaves Criptográficas

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

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 SAFEWEB RFB ÀS TERCEIRAS PARTES

As formas para a disponibilização do certificado da AC Safeweb 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 DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil;
- b) Diretório;
- c) Página *web*:
 - c.1) Cad. v2: <http://repositorio.acsafeweb.com.br/ac-safeweb/br/ac-safeweb/brv2.p7b>
 - c.2) Cad. v2: <http://repositorio2.acsafeweb.com.br/ac-safeweb/br/ac-safeweb/brv2.p7b>
 - c.3) Cad. v5: <http://repositorio.acsafeweb.com.br/ac-safeweb/br/ac-safeweb/brv5.p7b>
 - c.4) Cad. v5: <http://repositorio2.acsafeweb.com.br/ac-safeweb/br/ac-safeweb/brv5.p7b>
- 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 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 DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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 DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

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 Safeweb 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 chave privada de certificados emitidos conforme esta PC, é armazenada no repositório de certificados do sistema operacional utilizado pelo usuário no momento da emissão do certificado. 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 pode ser 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

Não se aplica.

6.2.2 CONTROLE "N DE M" PARA CHAVE PRIVADA

Não se aplica.

6.2.3 CUSTÓDIA (ESCROW) DE CHAVE PRIVADA

A AC Safeweb RFB não realiza custódia (*escrow*) de chaves privadas emitidas conforme esta PC.

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 Safeweb RFB não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3 Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, 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

Os titulares de certificado poderão optar por utilizar um *hardware* criptográfico, cartão inteligente ou token, para armazenar a 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 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 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 Safeweb 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 A1 da AC Safeweb RFB é de 1 (um) ano.

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 do repositório de certificados do sistema operacional para o 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 DE 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 dos certificados podem utilizar recursos adicionais de segurança como a definição de senhas para utilização e exportação das chaves privadas. A configuração e utilização destes recursos adicionais de proteção fica a critério do titular do certificado. No caso de utilização de senha, recomenda-se:

- 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 Safeweb 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

Não se aplica.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Não se aplica.

6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCRs geradas pela AC Safeweb 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 Safeweb 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 Safeweb 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 Safeweb 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: **2.16.76.1.2.1.51**;

c.2) O campo *PolicyQualifiers* contém o endereço *Web* onde se obtém a DPC AC Safeweb RFB: <http://repositorio.acsafeweb.com.br/ac-safeweb/brfb/dpc-acsafeweb/brfb.pdf>

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.acsafeweb.com.br/ac-safeweb/brfb/lcr-ac-safeweb/brfbv2.crl>

d.2) <http://repositorio2.acsafeweb.com.br/ac-safeweb/brfb/lcr-ac-safeweb/brfbv2.crl>

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

d.3) <http://repositorio.acsafeweb.com.br/ac-safeweb/brfb/lcr-ac-safeweb/brfbv5.crl>

d.4) <http://repositorio2.acsafeweb.com.br/ac-safeweb/brfb/lcr-ac-safeweb/brfbv5.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:

e.1) Raiz v2: <http://repositorio.acsafeweb.com.br/ac-safeweb/brfb/ac-safeweb/brfbv2.p7b>

e.2) Raiz v2: <http://repositorio2.acsafeweb.com.br/ac-safeweb/brfb/ac-safeweb/brfbv2.p7b>

e.3) Raiz v5: <http://repositorio.acsafeweb.com.br/ac-safeweb/brfb/ac-safeweb/brfbv5.p7b>

e.4) Raiz v5: <http://repositorio2.acsafeweb.com.br/ac-safeweb/brfb/ac-safeweb/brfbv5.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:

a.1) 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.

a.2) Não se aplica.

a.3) Não se aplica.

a.4) Não se aplica.

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*.

b) Para Certificados de Pessoa Jurídica:

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 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 ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente.
- 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 as 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 Safeweb 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.

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 Safeweb 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 = <Tipo de identificação utilizada>

OU = <CNPJ da AR que realizou a identificação>

OU = <Domínio do certificado> (Opcional)

OU = RFB e-CPF A1

OU = Secretaria da Receita Federal do Brasil – RFB

O = ICP-Brasil

C = BR

Onde:

I - 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.

II - 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 que realizou a identificação do titular.
- 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”.

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

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

b) CERTIFICADO e-CNPJ

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 que realizou a identificação>

L = <Cidade>

ST = <Sigla da unidade da federação>

O = ICP-Brasil

C = BR

Onde:

I - 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.

II - 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 que realizou a identificação do titular.

III - 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.

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

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

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

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 Safeweb 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:

Tabela 3

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 **2.16.76.1.2.1.51**.

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 Safeweb RFB: <http://repositorio.acsafeweb.com.br/ac-safewebrfb/dpc-acsafewebrfb.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 Safeweb 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 Safeweb RFB e sua criticalidade.

7.2.2.2 As LCRs da AC Safeweb 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 Safeweb RFB que assina a LCR; e
- b) "**CRL Number**", não crítica: contém um número sequencial para cada LCR emitida pela AC Safeweb 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 Safeweb 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 Safeweb 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

A AC Safeweb 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 e 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 Safeweb RFB mantém a versão corrente desta PC para consulta pública em seu repositório web, no endereço: <http://repositorio.acsafeweb.com.br/ac-safeweb/br/ac-safeweb-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 Safeweb 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 [2]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC Safeweb RFB.

10 DOCUMENTOS REFERENCIADOS

10.1 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 <https://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Tabela 4

Ref.	Nome do documento	Código
[1]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020.	DOC-ICP-04
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020.	DOC-ICP-03

11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.

RFC 2818, IETF - HTTP Over TLS, may 2000.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.