

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL CD SSL V5 A1

PC SERASA CD SSL V5 A1

<https://serasa.certificadodigital.com.br/>

V 3.0.

05 de maio de 2020



Sumário

CONTROLE DE ALTERAÇÕES	4
TABELA DE SIGLAS E ACRÔNIMOS	5
1 INTRODUÇÃO	7
1.1 Visão Geral.....	7
1.2 Nome do documento e identificação	7
1.3 Participantes da ICP-Brasil	8
1.4 Usabilidade do Certificado	8
1.5 Política de Administração.....	9
1.6 Definições e Acrônimos.....	9
2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO	11
2.1 Repositórios	11
2.2 Publicação de informações dos certificados	11
2.3 Tempo ou Frequência de Publicação	11
2.4 Controle de Acesso aos Repositórios	11
3 IDENTIFICAÇÃO E AUTENTICAÇÃO	11
3.1 Nomeação	11
3.2 Validação inicial de identidade	11
3.3 Identificação e autenticação para pedidos de novas chaves	12
3.4 Identificação e Autenticação para solicitação de revogação	12
4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	12
4.1 Solicitação do certificado	12
4.2 Processamento de Solicitação de Certificado	12
4.3 Emissão de Certificado.....	12
4.4 Aceitação de Certificado	12
4.5 Usabilidade do par de chaves e do certificado	12
4.6 Renovação de Certificados.....	12
4.7 Nova chave de certificado.....	12
4.8 Modificação de certificado	12
4.9 Suspensão e Revogação de Certificado	12
4.10 Serviços de status de certificado	13
4.11 Encerramento de atividades.....	13
4.12 Custódia e recuperação de chave.....	13
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES	13
5.1 Controles físicos	13
5.2 Controles Procedimentais	13
5.3 Controles de Pessoal.....	13
5.4 Procedimentos de Log de Auditoria	13
5.5 Arquivamento de Registros	14
5.6 Troca de chave	14
5.7 Comprometimento e Recuperação de Desastre	14
5.8 Extinção da AC	14
6 CONTROLES TÉCNICOS DE SEGURANÇA	14
6.1 Geração e Instalação do Par de Chaves.....	14
6.2 Proteção da Chave Privada e controle de engenharia do módulo criptográfico	15
6.3 Outros Aspectos do Gerenciamento do Par de Chaves	16
6.4 Dados de Ativação	17
6.5 Controles de Segurança Computacional	17
6.6 Controles Técnicos do Ciclo de Vida	17
6.7 Controles de Segurança de Rede	18
6.8 Carimbo de Tempo	18
7 PERFIS DE CERTIFICADO, LCR E OCSP	18
7.1 Perfil do certificado.....	18
7.2 Perfil de LCR.....	22
7.3 Perfil de OCSP	22
8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES	22
8.1 Frequência e circunstâncias das avaliações.....	22



8.2 Identificação/Qualificação do avaliador	22
8.3 Relação do avaliador com a entidade avaliada	22
8.4 Tópicos cobertos pela avaliação.....	22
8.5 Ações tomadas como resultado de uma deficiência.....	22
8.6 Comunicação dos resultados	22
9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS.....	23
9.1 Tarifas	23
9.2 Responsabilidade Financeira	23
9.3 Confidencialidade da informação do negócio	23
9.4 Privacidade da informação pessoal.....	23
9.5 Direitos de Propriedade Intelectual	23
9.6 Declarações e Garantias.....	23
9.7 Isenção de garantias	23
9.8 Limitações de responsabilidades.....	23
9.9 Indenizações	23
9.10 Prazo e Rescisão	23
9.11 Avisos individuais e comunicações com os participantes.....	23
9.12 Alterações	23
9.13 Solução de conflitos.....	24
9.14 Lei aplicável	24
9.15 Conformidade com a Lei aplicável	24
9.16 Disposições Diversas	24
9.17 Outras provisões	24
10 DOCUMENTOS REFERENCIADOS	24



CONTROLE DE ALTERAÇÕES

Versão da PC	Data da Alteração	Descrição da Alteração
3.0	05/05/2020	Adequação às resoluções 156 (07/02/2020) e 169 (17/04/2020)
2.0	30/08/2019	Adequação ao Resolução 151, de 30/05/2019.



TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	<i>Automatic Certificate Management Environment</i>
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	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
CONFAZ	Conselho Nacional de Política Fazendária
COSO	<i>Comitee of Sponsoring Organizations</i>
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
IETF PKIX	<i>Internet Engineering Task Force - Public-Key Infrastructured (X.509)</i>
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados



NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>On-line Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	<i>Proof of Possession</i>
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	<i>Simple Network Management Protocol</i>
SSL	<i>Secure Socket Layer</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	Uniform Resource Locator



1 INTRODUÇÃO

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

1.1 Visão Geral

1.1.1 Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras – AC integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Políticas de Certificado (PC).

1.1.2 Toda PC elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.1.3 São 12 (doze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

A1

A2

A3

A4

T3

T4

A CF-e-SAT OM-BR

b) Tipos de Certificados de Sigilo:

i. S1

ii. S2

iii. S3

iv. S4

1.1.4 Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5 Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6 Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

1.1.7 Certificados do tipo A CF-e-SAT só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico - SAT-CF-e, seguindo a regulamentação do CONFAZ.

1.1.8 Certificados do tipo Objeto Metrológico - OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro.

1.1.9 Outros tipos de certificado, além dos doze anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP -Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescentadas aos tipos de certificados aceitos pela ICP-Brasil.

1.1.10 Para certificados com propósito de uso EV SSL e EV CS devem ser observados os dispostos nos documentos EV SSL/CS Guidelines.

1.2 Nome do documento e identificação

1.2.1 Política de Certificado de Assinatura Digital, tipo A1, da AC SERASA CD SSL. O OID (Object Identifier) da PC AC SERASA CD SSL A1 é 2.16.76.1.2.1.69

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 SERASA CD SSL (Serasa S.A., com sede na Alameda dos Quinimuras, 187, São Paulo, SP, CEP 04068-900, CNPJ no 62.173.620/0001-80).

1.3.1.2 As práticas e procedimentos de certificação da AC SERASA CD SSL estão descritos na Declaração de Práticas de Certificação da AC SERASA CD SSL (a seguir designada simplesmente por "DPC-AC SERASA CD SSL").

1.3.2 Autoridades de Registro

1.3.2.1 A AC SERASA CD SSL disponibiliza em seu repositório: <https://serasa.certificadodigital.com.br/repositorio/>, os dados a seguir, referentes às Autoridades de Registro (AR) utilizadas pela AC para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

- 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

Os Titulares de Certificado de Assinatura Digital tipo A1 da AC SERASA CD SSL podem ser pessoas físicas ou jurídicas.

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

1.3.5.1 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 SERASA CD SSL, está publicado no repositório da AC: <https://serasa.certificadodigital.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 a aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

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 SERASA CD SSL 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 Certificados de tipos A1, A2, A3 e A4 são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Certificados de tipos S1, S2, S3 e S4 são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4.1.6 Certificados de tipos T3 e T4 são utilizados em aplicações mantidas por autoridades de carimbo do tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

1.4.1.7 Certificados de tipo A CF-e-SAT são utilizados exclusivamente em equipamentos para assinatura de Cupom Fiscal Eletrônico – CF-e por meio do Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico – SAT.



1.4.1.8 Certificados do tipo OM-BR são utilizados exclusivamente em equipamentos metrológicos regulamentados pelo Inmetro.

1.4.2 Uso proibitivo do certificado

Não se aplica.

1.5 Política de Administração

Dúvidas decorrentes da leitura desta PC e que não sejam respondidas mediante a leitura da página <https://serasa.certificadodigital.com.br/repositorio/> podem ser esclarecidas contatando:

Serasa S.A.
Alameda dos Quinimuras, 183, São Paulo, SP, CEP 04068-900
Tel. +55 11 2847-3643 / Fax. +55 11 2847-9755
Pessoa para contato: Giseli Mioti
E-mail: arcompliance@br.experian.com

1.5.1 Organização administrativa do documento

AC SERASA CD SSL

1.5.2 Contatos

Endereço: Alameda dos Quinimuras, 183, São Paulo, SP, CEP 04068-900
Telefone: +55 11 2847-3643
Fax: +55 11 2847-9755
Página web: <https://serasa.certificadodigital.com.br/repositorio/>
E-mail: arcompliance@br.experian.com
Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Giseli Mioti
Telefone: +55 11 2847-3643
E-mail: arcompliance@br.experian.com
Outros:

1.5.4 Procedimentos de aprovação da PC

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

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	<i>Automatic Certificate Management Environment</i>
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	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>



CN	<i>Common Name</i>
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
CONFAZ	Conselho Nacional de Política Fazendária
COSO	<i>Comitee of Sponsoring Organizations</i>
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	<i>Intrusion Detection System</i>
IEC	<i>International Electrotechnical Commission</i>
IETF PKIX	<i>Internet Engineering Task Force - Public-Key Infrastructured (X.509)</i>
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>On-line Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OM-BR	Objetos Metrológicos ICP-Brasil
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social



POP	<i>Proof of Possession</i>
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	<i>Simple Network Management Protocol</i>
SSL	<i>Secure Socket Layer</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SERASA CD SSL.

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

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SERASA CD SSL.

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 equipamento ou aplicação

3.2.4 Autenticação da identidade de um indivíduo

3.2.5 Informações não verificadas do titular do certificado

3.2.6 Validação das autoridades

3.2.7 Critérios para interoperação



3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 Identificação e autenticação para rotina de novas chaves

3.3.2 Identificação e autenticação para novas chaves após a revogação

3.4 Identificação e Autenticação para solicitação de revogação

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SERASA CD SSL.

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

Não se aplica.

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

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC SERASA CD SSL.

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

- 5.7.1 Procedimentos gerenciamento de incidente e comprometimento
- 5.7.2 Recursos computacionais, software, e/ou dados corrompidos
- 5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade
- 5.7.4 Capacidade de continuidade de negócio após desastre

5.8 Extinção da AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC. Definem também outros controles técnicos de segurança utilizados pela AC SERASA CD SSL e pelas ARs 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 for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1 Não se aplica.

6.1.1.1.2 Não se aplica.

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

- a) a instalação de hardware e software relacionados à mídia armazenadora do certificado selecionada 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 está 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 repositório protegido por senha e/ou identificação biométrica, cifrado por software.

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

6.1.1.6 A mídia de armazenamento da chave privada deverá assegurar, 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 deve estar 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.

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

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [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, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

Tabela 4 – 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

Nota: Não se aplica.

6.1.2 Entrega da chave privada à entidade

Item não aplicável.

6.1.3 Entrega da chave pública para emissor de certificado

A entidade titular do certificado, através de seu software de acionamento, disponibiliza para a entrega de sua chave pública à AC SERASA CD SSL, à solicitante ou a correspondente AR vinculada, a chave pública em formato PKCS#10, através de uma sessão segura SSL - Secure Socket Layer.

6.1.4 Entrega de chave pública da AC às terceiras partes

As formas para a disponibilização do certificado da AC SERASA CD SSL, e de todos os certificados da cadeia 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 ICPBRASIL;
- b) Diretório;
- c) Página Web da AC SERASA CD SSL (<https://serasa.certificadodigital.com.br/repositorio/>);
- d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1 Para certificados emitidos sob a cadeia da Autoridade Certificadora Raiz Brasileira 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 das entidades titulares de certificados adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

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

6.2 Proteção da 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.

6.2.1 Padrões e controle para módulo criptográfico



6.2.1.1 Neste item, quando cabíveis, devem ser especificados os padrões requeridos para os módulos de geração de chaves criptográficas, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.1.2 Este item da PC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado. Poderão ser indicados padrões de referência, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2 Controle “n de m” para chave privada

Item não aplicável.

6.2.3 Custódia (escrow) de chave privada

Não se aplica.

6.2.4 Cópia de segurança de chave privada

6.2.4.1 Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC SERASA CD SSL não pode manter cópia de segurança de chave privada de titular de certificado por ela emitido, segundo esta PC.

6.2.4.3 Em qualquer caso, a cópia de segurança será 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 da chave privada.

6.2.5 Arquivamento de chave privada

6.2.5.1 Não se aplica.

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

Não se aplica.

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 ao uso de senha no software de instalação do Certificado. A chave privada, juntamente com a sua senha de utilização, deve ser mantida em posse do titular do certificado.

6.2.9 Método de desativação de chave privada

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

6.2.10 Método de destruição de chave privada

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas da SERASA CD SSL, dos titulares de certificados de assinatura digital e as LCR 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 pública e privada

6.3.2.1 As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas 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 privadas correspondentes aos certificados emitidos pela SERASA CD SSL, segundo esta PC é de 1 (um) ano.

6.3.2.4 Não se aplica.

6.3.2.5 O período máximo de validade dos Certificados SSL/TLS é de até 825 (oitocentos e vinte cinco) dias, conforme princípios e critérios *Webtrust*.

6.4 Dados de Ativação

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

6.4.1 Geração e instalação dos dados de ativação

Os certificados de tipo A1 se utilizam, para geração e armazenamento do par de chaves e certificado, de repositório protegido por senha e/ou identificação biométrica, cifrado por software. No caso de ativação por senha, recomenda-se que as mesmas sejam criadas de forma aleatória, respeitando-se procedimentos básicos de segurança, tais como:

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

6.4.2 Proteção dos dados de ativação

Para a proteção dos dados de ativação da chave privada da entidade titular do certificado, no caso de ativação por senha, recomenda-se:

- a) Nunca fornecer senha a terceiros;
- b) Escolher senhas de 8 ou mais caracteres;
- c) Definir senhas com caracteres numéricos e alfanuméricos;
- d) Memorizar a senha e não escrevê-la.

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 SERASA CD SSL, 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 antispymware, 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 cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Não se aplica.

6.6.1 Controles de desenvolvimento de 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

Não se aplica.

6.7 Controles de Segurança de Rede

Não se aplica.

6.8 Carimbo de Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

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

7.1 Perfil do certificado

Todos os certificados emitidos pela AC SERASA CD SSL, segundo a PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC SERASA CD SSL, segundo a PC, implementam a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1 Neste item, a PC descreve todas as extensões de 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 deve conter o hash SHA-1 da chave pública da AC SERASA CD SSL;
- b) "Key Usage", crítica: configurados conforme disposto no item 7.1.2.7 deste documento;
- c) "Certificate Policies", não crítica: contém o OID desta PC e o endereço Web da DPC da AC SERASA CD SSL;
- d) "CRL Distribution Points", não crítica: contém o 2 (dois) endereços na Web onde se obtém a LCR correspondente.
- e) "Authority Information Access", não crítica: A primeira entrada deve conter o método de acesso id-ad-calssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada deve conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para certificados de autenticação de servidor (SSL/TLS). Todos os outros tipos de certificado podem conter essa segunda entrada. Essas extensões somente são aplicáveis para certificados de usuário final.

7.1.2.3 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:

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.

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.

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) 1 (um) campo otherName, obrigatório, para certificados vinculados ao



Documento RIC, contendo:

a.4) 1 (um) campo otherName, obrigatório para certificados digitais emitidos para servidor público e militar, contendo:

OID = 2.16.76.1.3.11 e conteúdo = nas primeiras 10 (dez) posições, o cadastro único do servidor público da ativa e militares da União constante no Sistema de Gestão de Pessoal (SIGPEPE) mantido pelo Ministério do Planejamento ou nos sistemas correlatos, no âmbito da esfera estadual e do Distrito Federal, e nos Sistemas de Gestão de Pessoal das Forças Armadas.

b) Para certificado de pessoa jurídica, 4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem: OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

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;

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

c) Para certificado de equipamento ou aplicação e OCSP:

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

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) Para certificados do tipo SSL/TLS, Campo dNSName, obrigatório, contendo um ou mais domínios pertencentes ou controlados pelo titular, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com os princípios e critérios WebTrust.

d) Não se aplica.

e) Não se aplica.

7.1.2.4 Os campos otherName definidos como obrigatórios pela ICP-Brasil estão 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 CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, 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, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;

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 emissor 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, 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.



7.1.2.5 Campos `otherName` adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC SERASA ACP.

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 devem obedecer os propósitos de uso e a criticidade conforme descrição abaixo :

a) para certificados de Assinatura de Código (`codeSigning`):

"Key Usage", crítica: somente o bit `digitalSignature` deve estar ativado;

"Extended Key Usage", não crítica: somente o `codeSigning` OID = 1.3.6.1.5.5.7.3.3 está presente;

b) para certificados de Autenticação de Servidor (SSL/TLS):

"Key Usage", crítica: somente os bits `digitalSignature`, `keyEncipherment` ou `keyAgreement` podem estar ativado;

"Extended Key Usage", não crítica: deve conter o propósito `server authentication` OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito `client authentication` OID = 1.3.6.1.5.5.7.3.2;

c) para certificados de Assinatura de Carimbo do Tempo:

"Key Usage", crítica: somente os bits `digitalSignature` e `nonRepudiation` devem estar ativado;

"Extended Key Usage", crítica: somente o propósito `timeStamping` OID = 1.3.6.1.5.5.7.3.8 deve estar presente. nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil. Esse OID não deve ser empregado em qualquer outro tipo de certificado;

d) para certificados de Assinatura A CF-e-SAT:

"Key Usage", crítica: deve conter o bit `digitalSignature` ativado, podendo conter os bits `keyAgreement` e `nonRepudiation` ativados;

"Extended Key Usage", não crítica: somente o propósito `client authentication` OID = 1.3.6.1.5.5.7.3.2 deve estar presente;

e) para certificados de Assinatura de Resposta OCSP:

"Key Usage", crítica: deve conter o bit `digitalSignature` ativado, podendo conter o bit `nonRepudiation` ativado;

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

f) para os demais certificados de Assinatura e/ou Proteção de e-Mail:

"Key Usage", crítica: deve conter o bit `digitalSignature` ativado, podendo conter os bits `keyEncipherment` e `nonRepudiation` ativados;

"Extended Key Usage", não crítica: no mínimo um dos propósitos `client authentication` OID

= 1.3.6.1.5.5.7.3.2 ou `E-mail protection` OID = 1.3.6.1.5.5.7.3.4 deve estar ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PC, em conformidade com a RFC 5280; e

g) para certificados de Sigilo:

"Key Usage", crítica: somente os bits `keyEncipherment` e `dataEncipherment` podem estar ativados.

7.1.3 Identificadores de algoritmo

Os certificados emitidos pela AC SERASA CD SSL são assinados com o uso dos seguintes algoritmos, conforme o padrão PKCS#1.

a) RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) ou RSA com SHA- 512 como função de hash (OID = 1.2.840.113549.1.1.13) nas cadeias V2 e V5 da ICP-Brasil;

7.1.4 Formatos de nome

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

C = BR

O = ICP-Brasil

OU = nome da AC emitente

OU = CNPJ da AR que realizou a identificação presencial; ou CNPJ da AR cujo AGR operou videoconferência para emissão do certificado; ou, ainda, a expressão "Renovação Eletrônica", para os casos de renovação online com certificado digital válido

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ); em um certificado de equipamento ou aplicação, o identificador CN deverá conter o URL correspondente ou o nome da aplicação

7.1.4.2 Não se aplica.



7.1.4.3 Não se aplica.

7.1.4.4 Certificado SSL

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

CN = <Nome do titular do certificado>

OU= <Nome do Requerente> <Protocolo Interno>

OU = Referência (indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica)

OU= Unidade (identifica grupo, área, divisão, seção ou qualquer outra identificação semelhante)

OU= Estado do Requerente.

OU= Sigla da unidade da federação.

OU = Código (número, nome ou sequência alfanumérica) CNPJ da AR emitente

OU =<Identificação da AC>

O = ICP-Brasil

C = BR

NOTA1: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

NOTA2: Caso qualquer um dos campos OU acima não seja utilizado, será grafado com o texto "(EM BRANCO)".

7.1.5 Restrições de nome

7.1.5.1 Não se aplica.

7.1.5.2 A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

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 7 - Caracteres especiais admitidos em nomes

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

7.1.6 OID (Object Identifier) da PC

O OID desta PC está descrito no item 1.2.1. Todo certificado emitido segundo esta PC contém, na extensão "Certificate Policies", o OID correspondente.

7.1.7 Uso da extensão "Policy Constraints"



Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC-AC SERASA CD SSL:
(<http://publicacao.certificadodigital.com.br/repositorio/dpc/declaracao-scd.pdf>);

7.1.9 Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC SERASA CD SSL, segundo a PC, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 Neste item, a PC são descritas todas as extensões de LCR utilizadas e sua criticalidade.

7.2.2.2 As LCR da AC SERASA CD SSL obedecem a ICP-Brasil e possuem as seguintes extensões obrigatórias:

a) Para LCRs emitidas sob a cadeia da Autoridade Certificadora Raiz Brasileira V5:

- i. "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC SERASA CD SSL que assina a LCR;
- ii. "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC SERASA CD SSL;

b) Para LCRs emitidas sob a cadeia da Autoridade Certificadora Raiz Brasileira V2:

- i. "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC SERASA CD SSL que assina a LCR;
- ii. "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC SERASA CD SSL;
- iii. "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia:
<http://www.certificadodigital.com.br/cadeias/serasarfbv2.p7b>.

c) Para LCRs emitidas sob a cadeia da Autoridade Certificadora Raiz Brasileira V1:

- i. "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC SERASA CD SSL que assina a LCR;
- ii. "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC SERASA CD SSL;

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

Os serviços de respostas OCSP da AC SERASA CD SSL implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

Os serviços de OCSP da AC SERASA CD SSL estão em conformidade com a RFC 6960.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SERASA CD SSL.

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

Nos itens seguintes são referidos os itens correspondentes da DPC da AC SERASA CD SSL. Os itens seguintes com requisitos especificados devem ser atendidos.

9.1 Tarifas

- 9.1.1 Tarifas de emissão e renovação de certificados**
- 9.1.2 Tarifas de acesso ao certificado**
- 9.1.3 Tarifas de revogação ou de acesso à informação de status**
- 9.1.4 Tarifas para outros serviços**
- 9.1.5 Política de reembolso**

9.2 Responsabilidade Financeira

- 9.2.1 Cobertura do seguro**
- 9.2.2 Outros ativos**
- 9.2.3 Cobertura de seguros ou garantia para entidades finais**

9.3 Confidencialidade da informação do negócio

- 9.3.1 Escopo de informações confidenciais**
- 9.3.2 Informações fora do escopo de informações confidenciais**
- 9.3.3 Responsabilidade em proteger a informação confidencial**

9.4 Privacidade da informação pessoal

- 9.4.1 Plano de privacidade**
- 9.4.2 Tratamento de informação como privadas**
- 9.4.3 Informações não consideradas privadas**
- 9.4.4 Responsabilidade para proteger a informação privadas**
- 9.4.5 Aviso e consentimento para usar informações privadas**
- 9.4.6 Divulgação em processo judicial ou administrativo**
- 9.4.7 Outras circunstâncias de divulgação de informação**

9.5 Direitos de Propriedade Intelectual

9.6 Declarações e Garantias

- 9.6.1 Declarações e Garantias da AC**
- 9.6.2 Declarações e Garantias da AR**
- 9.6.3 Declarações e garantias do titular**
- 9.6.4 Declarações e garantias das terceiras partes**
- 9.6.5 Representações e garantias de outros participantes**

9.7 Isenção de garantias

9.8 Limitações de 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

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

9.12.2 Mecanismo de notificação e períodos

Esta PC está disponível para a comunidade no endereço web <https://serasa.certificadodigital.com.br/repositorio/>.

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 SERASA CD SSL 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

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC SERASA CD SSL, 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, deverá ser verificada a compatibilidade entre a PC e a DPC da AC SERASA CD SSL.

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

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12

10.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

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