

IMPrensa OFICIAL DO ESTADO SA IMESP (AC IMPrensa OFICIAL SSL)

POLÍTICA DE CERTIFICADO DE ASSINATURA DIGITAL == TIPO A4 ==

VERSÃO 2.0 – 29/04/2020

HISTÓRICO DE VERSÕES

<i>Data</i>	<i>Versão</i>	<i>Observações</i>
15/12/2016	1.0	Redação Inicial
07/03/2019	1.1	Revisão
29/04/2020	2.0	Revisão

AVISO LEGAL

Copyright © Imprensa Oficial do Estado SA IMESP. Todos os direitos reservados.

Imprensa Oficial é uma marca registrada da Imprensa Oficial do Estado SA IMESP. Todas as restantes marcas, trademarks e service marks são propriedade dos seus respectivos detentores.

É expressamente proibida a reprodução, total ou parcial, do conteúdo deste documento, sem prévia autorização escrita emitida pela Imprensa Oficial.

Qualquer dúvida ou pedido de informação relativamente ao conteúdo deste documento deverá ser dirigido a certificacao@imprensaoficial.com.br.

CONTEÚDO

1.	Introdução	11
1.1.	Visão Geral	11
1.2.	Nome do documento e Identificação	11
1.3.	participantes da icp-brasil	11
1.3.1	Autoridades Certificadoras	11
1.3.2	Autoridades de Registro	12
1.3.3	Titulares do certificado	12
1.3.4	partes confiáveis.....	12
1.3.5	Prestador de Serviço de Suporte	12
1.4.	usabilidade do certificado	12
1.4.1	Uso apropriado do certificado	12
1.4.2	Uso proibitivo do certificado.....	13
1.5.	Política de Administração	13
1.5.1	Organização administrativa do documento	13
1.5.2	Contatos	13
1.5.3	Pessoa que determina a adequabilidade da DPC com a PC	13
1.5.4	Procedimentos de aprovação da DPC	13
1.6	Definições e Acrônimos	14
2.	Responsabilidades de publicação e repositório	16
2.1.	Repositórios.....	16
2.2.	PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS	16
2.3.	TEMPO E FREQUÊNCIA DE PUBLICAÇÃO	16
2.4.	CONTROLE DE ACESSO AOS REPOSITÓRIOS	16
3.	Identificação e Autenticação.....	16
3.1.	Nomeação.....	16
3.1.1	Tipos de nomes	16
3.1.2	Necessidade de nomes serem significativos.....	16
3.1.3	Anonimato ou Pseudônimo dos Titulares de certificados	16
3.1.4	Regras para interpretação de vários nomes	16
3.1.5	Unicidade de nomes.....	16
3.1.6	Procedimento para resolver disputa de nomes	16
3.1.7	Reconhecimento, autenticação e papel de marcas registradas	16
3.2.	Validação inicial de identidade	16
3.2.1	Método para comprovar a posse da chave privada.....	16
3.2.2	Autenticação da identidade de uma organização	16
3.2.3	Autenticação da identidade de um equipamento ou aplicação	16

3.2.4	Autenticação da identidade de um indivíduo	16
3.2.5	Informações não verificadas do titular do certificado.....	16
3.2.6	Validação das autoridades.....	16
3.2.7	Critérios para interoperação	16
3.3.	Identificação e autenticação para pedidos de novas chaves.....	16
3.3.1	Identificação e autenticação para rotina de novas chaves	16
3.3.2	Identificação e autenticação para novas chaves após a revogação	16
3.4.	Identificação e Autenticação para solicitação de revogação	17
4.	Requisitos operacionais do Ciclo de Vida do certificado	17
4.1.	Solicitação de Certificado.....	17
4.1.1	Quem pode submeter uma solicitação de certificado.....	17
4.1.2	Processo de registro e responsabilidades.....	17
4.2.	Processamento de solicitação de certificado	17
4.2.1	Execução das funções de identificação e autenticação	17
4.2.2	Aprovação ou rejeição de pedidos de certificado	17
4.2.3	Tempo par processar a solicitação de certificado.....	17
4.3.	Emissão de certificado	17
4.3.1	Ações da AC durante a emissão de um certificado	17
4.3.2	Notificações para o titular do certificado pela AC na emissão do certificado	17
4.4.	Aceitação de Certificado	17
4.4.1	Conduta sobre a aceitação do certificado.....	17
4.4.2	Publicação do certificado da AC	17
4.4.3	Notificação de emissão do certificado pela AC Raiz para outras entidades.....	17
4.5.	Usabilidade do par de chaves e do certificado.....	18
4.5.1	Usabilidade da Cave privada e do certificado do titular	18
4.5.2	Usabilidade da chave publica e do certificado das partes confiáveis	18
4.6.	Renovação de certificados.....	18
4.6.1	CIRCUNSTÂNCIAS PARA RENOVAÇÃO DE CERTIFICADOS.....	18
4.6.2	QUEM PODE SOLICITAR A RENOVAÇÃO.....	18
4.6.3	PROCESSAMENTO DE REQUISIÇÃO PARA RENOVAÇÃO DE CERTIFICADOS	18
4.6.4	NOTIFICAÇÃO PARA NOVA EMISSÃO DE CERTIFICADO PARA O TITULAR	18

4.6.5 CONDOTA CONSTITUINDO A ACEITAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO	18
4.6.6 PUBLICAÇÃO DE UMA RENOVAÇÃO DE UM CERTIFICADO PELA AC..	18
4.6.7 NOTIFICAÇÃO DE EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	18
4.7. Nova chave de certificado	18
4.7.1 CIRCUNSTÂNCIAS PARA NOVA CHAVE DE CERTIFICADO	18
4.7.2 QUEM PODE REQUISITAR A CERTIFICAÇÃO DE UMA NOVA CHAVE PÚBLICA	18
4.7.3 PROCESSAMENTO DE REQUISIÇÃO DE NOVAS CHAVES DE CERTIFICADO	18
4.7.4 NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR	18
4.7.5 CONDOTA CONSTITUINDO A ACEITAÇÃO DE UMA NOVA CHAVE CERTIFICADA.....	18
4.7.6 PUBLICAÇÃO DE UMA NOVA CHAVE CERTIFICADA PELA AC	18
4.7.7 NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	18
4.8. Modificação de certificado	18
4.8.1 CIRCUNSTÂNCIAS PARA MODIFICAÇÃO DE CERTIFICADO	18
4.8.2 QUEM PODE REQUISITAR A MODIFICAÇÃO DE CERTIFICADO	18
4.8.3 PROCESSAMENTO DE REQUISIÇÃO DE MODIFICAÇÃO DE CERTIFICADO	18
4.8.4 NOTIFICAÇÃO DE EMISSÃO DE NOVO CERTIFICADO PARA O TITULAR	18
4.8.5 CONDOTA CONSTITUINDO A ACEITAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO	18
4.8.6 PUBLICAÇÃO DE UMA MODIFICAÇÃO DE CERTIFICADO PELA AC.....	18
4.8.7 NOTIFICAÇÃO DE UMA EMISSÃO DE CERTIFICADO PELA AC PARA OUTRAS ENTIDADES	18
4.9. Suspensão e Revogação de Certificado.....	18
4.9.1 Circunstâncias para revogação	19
4.9.2 Quem pode solicitar revogação	19
4.9.3 Procedimento para solicitação de revogação	19
4.9.4 Prazo para solicitação de revogação	19
4.9.5 Tempo em que a AC deve processar o pedido de revogação	19
4.9.6 Requisitos de verificação de revogação para as partes confiáveis ..	19
4.9.7 Frequência de emissão de LCR	19
4.9.8 Latência máximo para a LCR.....	19
4.9.9 Disponibilidade para revogação/verificação de status on-line.....	19
4.9.10 Requisitos para verificação de revogação on-line	19

4.9.11	Outras formas disponíveis para divulgação de revogação.....	19
4.9.12	Requisitos especiais para o caso de comprometimento de chave .	19
4.9.13	Circunstâncias para suspensão	19
4.9.14	Quem pode solicitar suspensão.....	19
4.9.15	Procedimento para solicitação de suspensão.....	19
4.9.16	Limites no período de suspensão.....	19
4.10.	SERVIÇOS DE STATUS DE CERTIFICADO	19
4.10.1	CARACTERÍSTICAS OPERACIONAIS	19
4.10.2	DISPONIBILIDADE DOS SERVIÇOS.....	19
4.10.3	FUNCIONALIDADES OPERACIONAIS.....	19
4.11.	ENCERRAMENTO DE ATIVIDADES	19
4.12.	CUSTÓDIA E RECUPERAÇÃO DE CHAVE.....	19
4.12.1	POLÍTICA E PRÁTICAS DE CUSTÓDIA E RECUPERAÇÃO DE CHAVE.....	19
4.12.2	POLÍTICA E PRÁTICAS DE ENCAPSULAMENTO E RECUPERAÇÃO DE CHAVE DE SESSÃO	19
5.	Controles operacionais, gerenciamento e de instalações	19
5.1.	Controles Físicos.....	19
5.1.1	Acesso físico	20
5.1.2	Energia e ar condicionado	20
5.1.3	Exposição à água	20
5.1.4	Prevenção e proteção contra incêndio	20
5.1.5	Armazenamento de mídia.....	20
5.1.6	Destruição de lixo	20
5.1.7	Instalações de segurança (backup) externas (off-site) para AC	20
5.2.	Controles Procedimentais	20
5.2.1	Perfis qualificados	20
5.2.2	Número de pessoas necessário por tarefa.....	20
5.2.3	Identificação e autenticação para cada perfil	20
5.2.4	Funções que requerem separação de deveres	20
5.3.	Controles de Pessoal.....	20
5.3.1	Antecedentes, qualificação, experiência e requisitos de idoneidade	20
5.3.2	Procedimentos de verificação de antecedentes	20
5.3.3	Requisitos de treinamento.....	20
5.3.4	Frequência e requisitos para reciclagem técnica	20
5.3.5	Frequência e sequência de rodízio de cargos.....	20
5.3.6	Sanções para ações não autorizadas	20

5.3.7	Requisitos para contratação de pessoal.....	20
5.3.8	Documentação fornecida ao pessoal	20
5.4.	Procedimentos de Log de Auditoria	20
5.4.1	Tipos de eventos registrados.....	20
5.4.2	Frequência de auditoria de registros (logs).....	20
5.4.3	Período de retenção para registros (logs) de auditoria.....	20
5.4.4	Proteção de registro (log) de auditoria	20
5.4.5	Procedimentos para cópia de segurança (backup) de registro (log) de auditoria	20
5.4.6	Sistema de coleta de dados de auditoria (interno ou externo)	20
5.4.7	Notificação de agentes causadores de eventos	20
5.4.8	Avaliações de vulnerabilidade	20
5.5.	Arquivamento de Registros.....	21
5.5.1	Tipos de registros arquivados.....	21
5.5.2	Período de retenção para arquivo	21
5.5.3	Proteção de arquivo.....	21
5.5.4	Procedimentos para cópia de arquivo	21
5.5.5	Requisitos para datação (time-stamping) de registros	21
5.5.6	Sistema de coleta de dados de arquivo (interno e externo)	21
5.5.7	Procedimentos para obter e verificar informação de arquivo.....	21
5.6.	Troca de chave	21
5.7.	Comprometimento e Recuperação de Desastre.....	21
5.7.1	Recursos computacionais, software, e dados corrompidos.....	21
5.7.2	Procedimentos no caso de comprometimento de chave privada de entidade	21
5.7.3	Capacidade de continuidade de negócio após desastre	21
5.8.	Extinção da AC.....	21
6.	Controles Técnicos de Segurança	21
6.1.	Geração e Instalação do Par de Chaves.....	21
6.1.1	Geração do par de chaves	21
6.1.2	Entrega da chave privada à entidade	22
6.1.3	Entrega da chave pública para emissor de certificado.....	22
6.1.4	Entrega da chave pública da AC às terceiras partes	23
6.1.5	Tamanhos de chave	23
6.1.6	Geração de parâmetros de chaves assimétricas e Verificação da qualidade dos parâmetros	23
6.1.7	PROPÓSITOS DE USO DE CHAVE (CONFORME O CAMPO "KEY USAGE" NA X.509V3)	23

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico	23
6.2.1. Padrões para módulo criptográfico	23
6.2.3. Controle “n de m” para chave privada	23
6.2.3 Custódia (escrow) de chave privada	23
6.2.4 Cópia de segurança (backup) de chave privada	24
6.2.5 Arquivamento de chave privada	24
6.2.6 Inserção de chave privada em módulo criptográfico	24
6.2.7 armazenamento de chave privada em módulo criptográfico	24
6.2.8 Método de ativação de chave privada	24
6.2.9. Método de desativação de chave privada	24
6.2.10 Método de destruição de chave privada	24
6.3. Outros Aspectos do Gerenciamento do Par de Chaves	25
6.3.1 Arquivamento de chave pública	25
6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada	25
6.4. Dados de Ativação	25
6.4.1 Geração e instalação dos dados de ativação	25
6.4.2 Proteção dos dados de ativação	25
6.4.3 Outros aspectos dos dados de ativação	25
6.5. Controles de Segurança Computacional	26
6.5.1 Requisitos técnicos específicos de segurança computacional	26
6.5.2 Classificação da segurança computacional	26
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	26
6.6.1 controles de desenvolvimento de sistema	26
6.6.2. controles de gerenciamento de segurança	26
6.6.3. controles de segurança de ciclo de vida	26
6.6.4. controles na geração de LCR	26
6.7. Controles de Segurança de Rede	26
6.8. carimbo do tempo	27
7. Perfis de Certificado, LCR e oosp	27
7.1. Perfil do Certificado	27
7.1.1 Número de versão	27
7.1.2 Extensões de certificado	27
7.1.3. Identificadores de algoritmo	30
7.1.4. Formatos de nome	30
7.1.5 Restrições de nome	31

7.1.6	OID (Object Identifier) de Política de Certificado.....	32
7.1.7	Uso da extensão "Policy Constraints"	32
7.1.8	Sintaxe e semântica dos qualificadores de política	32
7.1.9	Semântica de processamento para extensões críticas de PC	32
7.2.	Perfil de LCR	32
7.2.1	Número(s) de versão.....	32
7.2.2	Extensões de LCR e de suas entradas.....	32
7.3.	PERFIL DE OCSP	33
7.3.1.	número(s) de versão	33
7.3.2.	extensões de ocsp	33
8.	Auditoria de conformidade e outras avaliações	33
8.1.	frequência e circunstâncias das avaliações.....	33
8.2.	Identificação/qualificação do avaliador	33
8.3.	relação do avaliador com a entidade avaliada	33
8.4.	tópicos cobertos pela avaliação	33
8.5.	ações tomadas como resultado de uma deficiência.	33
8.6.	Comunicação dos resultados	33
9.	outros negócios e assuntos jurídicos	33
9.1.	tarifas.....	33
9.1.1.	Tarifas de emissão e renovação de certificados	33
9.1.2.	Tarifas de acesso ao certificado	33
9.1.3.	Tarifas de revogação ou de acesso à informação de status	33
9.1.4.	Tarifas para outros serviços.....	33
9.1.5.	Política de reembolso	33
9.2.	Responsabilidades financeira	34
9.2.1.	Cobertura do seguro	34
9.2.2.	Outros ativos.....	34
9.2.3.	Cobertura de seguros ou garantia para entidades finais.....	34
9.3.	CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	34
9.3.1.	Escopo de informações confidenciais.....	34
9.3.2.	Informações fora do escopo de informações confidenciais.....	34
9.3.3.	Responsabilidade em proteger a informação confidencial.....	34
9.4.	privacidade da informação pessoal	34
9.4.1.	Plano de privacidade	34
9.5.	DIREITOS DE PROPRIEDADE INTELECTUAL.....	34
9.6.	DECLARAÇÕES E GARANTIAS	34
9.6.1.	Declarações e garantias da AC	34

9.6.2. Declarações e garantias da AR.....	34
9.6.3. Declarações e garantias do titular.....	34
9.6.4. Declarações e garantias das terceiras partes.....	34
9.6.5. Representações e garantias de outros participantes.....	34
9.7. ISENÇÃO DE GARANTIAS.....	34
9.8. LIMITAÇÕES DE RESPONSABILIDADES.....	34
9.9. INDENIZAÇÕES.....	34
9.10. PRAZO E RESCISÃO.....	35
9.10.1. PRAZO.....	35
9.10.2. TÉRMINO.....	35
9.10.3. EFEITO DA RESCISÃO E SOBREVIVÊNCIA.....	35
9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES....	35
9.12. ALTERAÇÕES.....	35
9.12.1. PROCEDIMENTO PARA EMENDAS.....	35
9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS.....	35
9.12.3. CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO.....	35
9.13. SOLUÇÃO DE CONFLITOS.....	35
9.14. LEI APLICÁVEL.....	35
9.15. CONFORMIDADE COM A LEI APLICÁVEL.....	35
9.16. DISPOSIÇÕES DIVERSAS.....	35
9.16.1. ACORDO COMPLETO.....	35
9.16.2. CESSÃO.....	35
9.16.3. INDEPENDÊNCIA DE DISPOSIÇÕES.....	35
9.16.4. EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS).....	35
9.17. OUTRAS PROVISÕES.....	35
10. Documentos Referenciados.....	36

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1 Esta “Política de Certificado” (PC) descreve as políticas de certificação de certificados de Assinatura Digital de Tipo A4 da Autoridade Certificadora Imprensa Oficial SSL na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1.2. A estrutura desta PC está baseada no DOC-ICP-04 do Comitê Gestor da ICP-Brasil – Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil e na RFC n.º 2527 (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*).

1.1.3. O tipo de certificado emitido sob esta PC é o Tipo A4.

1.1.4. Não se aplica.

1.1.5. Esta PC refere-se exclusivamente a certificados de Pessoa Física, de Pessoa Jurídica, de Equipamento Servidor e Aplicação do Tipo A4 da Autoridade Certificadora Imprensa Oficial SSL.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.1.8. Não se aplica.

1.1.9. Não se aplica.

1.1.10. Para certificados com propósito de uso EV SSL deve ser observado o disposto no documento EV SSL Guidelines.”

1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1. Esta PC é designada de “Política de Certificado de Assinatura Digital Tipo A4 da Autoridade Certificadora Imprensa Oficial SSL” e referida como “PC A4 da AC IMPRENSA OFICIAL SSL”. Esta PC descreve os procedimentos e práticas da AC IMPRENSA OFICIAL SSL e os usos relacionados ao certificado de Assinatura Digital do tipo A4. O OID (object identifier) desta PC é 2.16.76.1.2.4.42.

1.2.2. Não se aplica.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1. Esta PC refere-se exclusivamente à AC IMPRENSA OFICIAL SSL no âmbito da ICP-Brasil.

1.3.1.2. As práticas e procedimentos de certificação da AC IMPRENSA OFICIAL SSL estão descritos na Declaração de Práticas de Certificação da AC IMPRENSA OFICIAL SSL (DPC da AC IMPRENSA OFICIAL SSL).

1.3.2 AUTORIDADES DE REGISTRO

1.3.2.1. Os dados seguintes, referentes às Autoridades de Registro – AR utilizadas pela AC IMPRENSA OFICIAL SSL para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC IMPRENSA OFICIAL SSL (<http://certificadodigital.imprensaoficial.com.br/repositorio/ac/imespssl>):

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

1.3.3 TITULARES DO CERTIFICADO

Os titulares de certificado de assinatura do Tipo A4 podem ser pessoas físicas ou jurídicas, equipamentos ou aplicações.

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 PRESTADOR DE SERVIÇO DE SUPORTE

1.3.5.1. São também publicados em serviço de diretório e/ou em página web da AC IMPRENSA OFICIAL SSL (<http://certificadodigital.imprensaoficial.com.br/repositorio/ac/imespssl>):

- a) relação de todos os Prestadores de Serviço de Suporte – PSS;
- b) relação de todos os Prestadores de Serviços Biométricos – PSBIOS;
- c) relação de todos os Prestadores de Serviços de Confiança-PSC

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, autenticação de seu titular e de aplicações e identificação de equipamentos.

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. A AC IMPRENSA OFICIAL SSL leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves,

procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados – LCR e extensão do período de validade do certificado.

1.4.1.4. Os certificados emitidos sob esta PC são apropriados ao uso, por exemplo, nas aplicações abaixo:

- Assinatura digital em correio eletrônico;
- Acesso a aplicações disponibilizadas pela Receita Federal do Brasil, ou por qualquer outro órgão da Administração Pública Direta ou Indireta, que aceitem este certificado;
- Software de assinatura elaborado em parceria com outros órgãos, entidades ou empresas;
- Transações eletrônicas e transações on-line;
- Redes privadas virtuais (VPN).

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

Os certificados emitidos sob esta PC devem apenas ser usados na medida em que seja consistente com a lei aplicável.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Imprensa Oficial SSL

1.5.2 CONTATOS

Endereço: Rua da Mooca, 1921 – Mooca – São Paulo, SP

Telefone: (55 11) 0800 0123401

Telefone: (55 11) 2799 9800

Página web: www.imprensaoficial.com.br

E-mail: certificacao@imprensaoficial.com.br

1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

Nome: Roseli Ramalho de Jesus Caccas

Telefone: (55 11) 2799 9805

E-mail: certificacao@imprensaoficial.com.br

1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA DPC

Esta DPC é aprovada pelo ITI.

Os procedimentos de aprovação da DPC da AC IMPRENSA OFICIAL SSL são estabelecidos a critério do CG da ICP-Brasil.

1.6 DEFINIÇÕES E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	<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	<i>Control Objectives for Information and Related Technology</i>
COSO	<i>Comitee of Sponsoring Organizations</i>
CONFAZ	Conselho Nacional de Política Fazendária
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 Metroológicos 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
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
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

- 2.1. REPOSITÓRIOS**
- 2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS**
- 2.3. TEMPO E 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 IMPRENSA OFICIAL SSL.

3.1. NOMEAÇÃO

- 3.1.1 TIPOS DE NOMES**
- 3.1.2 NECESSIDADE DE NOMES SEREM SIGNIFICATIVOS**
- 3.1.3 ANONIMATO OU PSEUDÔNIMO DOS TITULARES DE CERTIFICADOS**
- 3.1.4 REGRAS PARA INTERPRETAÇÃO DE VÁRIOS 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 DA CHAVE PRIVADA**
- 3.2.2 AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO**
- 3.2.3 AUTENTICAÇÃO DA IDENTIDADE DE UM 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 IMPRENSA OFICIAL SSL.

4.1. SOLICITAÇÃO DE CERTIFICADO

4.1.1 QUEM PODE SUBMETER UMA SOLICITAÇÃO DE CERTIFICADO

4.1.2 PROCESSO DE REGISTRO E RESPONSABILIDADES

4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

4.2.1 EXECUÇÃO DAS FUNÇÕES DE IDENTIFICAÇÃO E AUTENTICAÇÃO

4.2.2 APROVAÇÃO OU REJEIÇÃO DE PEDIDOS DE CERTIFICADO

4.2.3 TEMPO PAR 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 DA 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 CAVE 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 MÁXIMO 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 são referidos os itens correspondentes da DPC da AC IMPRENSA OFICIAL SSL.

5.1. CONTROLES FÍSICOS

- 5.1.1 ACESSO FÍSICO
- 5.1.2 ENERGIA E AR CONDICIONADO
- 5.1.3 EXPOSIÇÃO À ÁGUA
- 5.1.4 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO
- 5.1.5 ARMAZENAMENTO DE MÍDIA
- 5.1.6 DESTRUIÇÃO DE LIXO
- 5.1.7 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 (LOGS)
- 5.4.3 PERÍODO DE RETENÇÃO PARA REGISTROS (LOGS) DE AUDITORIA
- 5.4.4 PROTEÇÃO DE REGISTRO (LOG) DE AUDITORIA
- 5.4.5 PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO (LOG) DE AUDITORIA
- 5.4.6 SISTEMA DE COLETA DE DADOS DE AUDITORIA (INTERNO OU EXTERNO)
- 5.4.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS
- 5.4.8 AVALIAÇÕES DE VULNERABILIDADE

5.5. ARQUIVAMENTO DE REGISTROS

5.5.1 TIPOS DE REGISTROS ARQUIVADOS

5.5.2 PERÍODO DE RETENÇÃO PARA ARQUIVO

5.5.3 PROTEÇÃO DE ARQUIVO

5.5.4 PROCEDIMENTOS PARA CÓPIA DE ARQUIVO

5.5.5 REQUISITOS PARA DATAÇÃO (TIME-STAMPING) DE REGISTROS

5.5.6 SISTEMA DE COLETA DE DADOS DE ARQUIVO (INTERNO E EXTERNO)

5.5.7 PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

5.6. TROCA DE CHAVE

5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

5.7.1 RECURSOS COMPUTACIONAIS, SOFTWARE, E DADOS CORROMPIDOS

5.7.2 PROCEDIMENTOS NO CASO DE COMPROMETIMENTO DE CHAVE PRIVADA DE ENTIDADE

5.7.3 CAPACIDADE DE CONTINUIDADE DE NEGÓCIO APÓS DESASTRE

5.8. EXTINÇÃO DA AC

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1. O par de chaves criptográficas é gerado pelo titular do certificado, quando este for uma pessoa física. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração do par 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. A geração do par de chaves criptográficas ocorre, no mínimo, utilizando software CSP (Cryptographic Service Provider) existente na estação do solicitante, sendo a chave privada armazenada nesse software. A chave privada poderá ser exportada e armazenada (cópia de segurança) em mídia externa – ficheiro, disquete, token ou cartão inteligente – e protegida por senha de acesso.

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

6.1.1.4. Ao ser gerada, a chave privada do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A4.

6.1.1.5. O usuário deve assegurar que 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. O meio de armazenamento da chave privada utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

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

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

6.1.1.8. O tipo de certificado emitido pela AC IMPRENSA OFICIAL SSL descrito nesta PC é o A4.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A4	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 definido do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.4 ENTREGA DA CHAVE PÚBLICA DA AC ÀS TERCEIRAS PARTES

A AC IMPRENSA OFICIAL SSL disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, de entre outras, em formato PKCS#7, através de endereço Web:

<HTTP://CERTIFICADODIGITAL.IMPRESAOFICIAL.COM.BR/REPOSITORIO/AC/IMESPSSL>

6.1.5 TAMANHOS DE CHAVE

6.1.5.1. O tamanho mínimo das chaves criptográficas associadas aos certificados emitidos pela AC IMPRENSA OFICIAL SSL é 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A4 da ICP-Brasil está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados adotam, o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

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

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

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

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura sem o consentimento do titular do certificado.

6.2.4 CÓPIA DE SEGURANÇA (BACKUP) DE CHAVE PRIVADA

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

6.2.4.2. A AC IMPRENSA OFICIAL SSL não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital.

6.2.4.3. Em qualquer caso, a cópia de segurança deverá ser armazenada, cifrada, por algoritmo simétrico 3-DES, IDEA, SAFER+ ou outros aprovados 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. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1. A AC IMPRENSA OFICIAL SSL não arquiva cópias de chaves privadas de assinatura digital de titulares de certificados.

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

6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

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

6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

Cada titular de certificado deve definir procedimentos necessários para a ativação da sua chave privada.

6.2.9. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

Cada titular de certificado deve definir procedimentos necessários para a desativação da sua chave privada.

6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Cada titular de certificado deve 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 dos titulares de certificados de assinatura digital emitidos pela AC IMPRENSA OFICIAL SSL permanecem armazenadas após a expiração dos certificados correspondentes, pelo período legalmente estabelecido, 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 de assinatura dos respectivos titulares de certificados são utilizadas apenas durante 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 das 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 validade admitido para certificados de Assinatura Digital Tipo A4 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 será de até 825 (oitocentos e vinte cinco) dias, conforme princípios e critérios Webtrust.

6.4. DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

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

6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar pela sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, tais como:

- a) Controle de acesso lógico ao sistema operacional;
- b) Exigência de uso de senhas fortes;
- c) Diretivas de senha e de bloqueio de conta;
- d) Antivírus, antitrojan e antispysware, instalados, atualizados e habilitados;
- e) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;
- f) Sistema operacional mantido atualizado, com aplicação de correções necessárias (patches, hotfix, etc.);
- g) 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

Antes de publicadas, todas as LCR geradas pela AC são verificadas 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, LCR E OCSP

7.1. PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC IMPRENSA OFICIAL SSL 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 IMPRENSA OFICIAL SSL implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 EXTENSÕES DE CERTIFICADO

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

7.1.2.2. Extensões Obrigatórias:

- a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC IMPRENSA OFICIAL SSL;
- b) "Key Usage", crítica: somente os bits digitalSignature, nonRepudiation e keyEncipherment estão ativados;
- c) "Certificate Policies", não crítica contém:
 - O OID desta PC: 2.16.76.1.2.4.43Os campos policyQualifiers contém o endereço Web da DPC AC IMPRENSA OFICIAL SSL:
https://certificadodigital.imprensaoficial.com.br/media/files/ac_imprensa_oficial_ssl_dpc_v2_0.pdf
- d) "CRL Distribution Points", não crítica, contém os endereços Web onde se obtém a LCR correspondente:

<http://certificadodigital.imprensaoficial.com.br/repositorio/ac/imespssl>
<http://www.digitaltrust.com.br/repositorio/IMESPSSL/ACIMESPSSL.crl>

<http://repositorio.icpbrasil.gov.br/lcr/IMESP/ACIMESPSSL.crl>

- e) "Authority Information Access", não crítica, contém:
o endereço web onde se poderá obter a cadeia de certificação através do link:
<http://certificadodigital.imprensaoficial.com.br/repositorio/ac/imespssl>

o endereço web onde se pode aceder ao serviço OCSP, através do <http://io-ocsp-icpbr.imprensaoficial.com.br>

7.1.2.3. Os certificados emitidos pela AC IMPRENSA OFICIAL SSL possuem a extensão "Subject Alternative Name", não crítica e com os seguintes formatos:

- a) Não aplicável.
- b) Não aplicável.
- c) Para certificado de equipamento ou aplicação:
 - c.1) 4 (quatro) campos otherName, obrigatórios, contendo:
 - i. 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.
 - ii. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica.
 - iii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado.
 - iv. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaa; 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) do responsável; 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) Quando os certificados de equipamento forem emitidos para servidores de Domain Controller, adicionalmente, irão conter um campo otherName com OID = 1.3.6.1.4.1.311.25.1 e conteúdo = identificador (Globally Unique Identifier – GUID) do Domain Controller;
 - c.3) Campo DNS Name, contendo o nome do domínio.
- d) Não aplicável.
- e) Não aplicável.

7.1.2.4. Os campos `otherName`, definidos como obrigatórios, estão de acordo com as seguintes especificações:

- a) O conjunto de informações definido em cada campo `otherName` é armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, ou PRINTABLE STRING, com exceção do campo UPN que possui uma cadeia de caracteres do tipo ASN.1 UTF8 STRING.
- b) Quando os números de NIS (PIS, PASEP ou CI), RG, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes são integralmente preenchidos com caracteres "zero".
- c) Se o número do RG não estiver disponível, não é preenchido o campo de órgão emissor e UF. O mesmo ocorre para o campo do 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 pelo conselho de classe profissional.
- e) Todas as informações de tamanho variável, referentes a números, tal como RG, são preenchidos com caracteres "zero" à 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, sendo utilizados 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 municípios e UF do Título de Eleitor.
- g) Apenas 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.

7.1.2.5. Campos `otherName` adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidos pela AC IMPRENSA OFICIAL SSL, podem ser utilizados com OID atribuídos ou aprovados pela AC-Raiz.

7.1.2.6. Os outros campos que compõem a extensão "Subject Alternative Name" podem 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 :

- 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;

7.1.3. IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC IMPRENSA OFICIAL SSL são assinados utilizando o algoritmo RSA com SHA-256 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, constante do campo "Subject", adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = <Identificador: nome, nome da AC, número ou suas combinações, ou sequência alfanumérica>

OU = <CNPJ da AR onde ocorreu a identificação presencial>

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

E = <endereço de email>

CN = <Nome do titular> do certificado de pessoa física; em um certificado de pessoa jurídica é o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

O campo DN pode apresentar outros campos "OU". Caso qualquer um dos campos OU não seja utilizado, o mesmo não será apresentado no DN.

Num certificado de pessoa jurídica, o identificador CN contém a denominação da razão social correspondente.

Num certificado de equipamento ou aplicação, o identificador CN contém o URL correspondente ou o nome da aplicação, e não contém o campo E. Será escrito o nome até o limite do tamanho do campo disponível.

O campo Locality (L), opcional, com conteúdo correspondente ao nome da cidade onde a empresa/titular está localizada/o. O campo deve ser preenchido sem acentos nem abreviaturas.

O campo State or Province Name (ST), opcional, com conteúdo correspondente à sigla do estado onde a empresa/titular está localizada/o.

7.1.4.2. Não se aplica.

7.1.4.3. Não se aplica.

7.1.4.4. O certificado digital emitido para autenticação de servidor (SSL/TLS) deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = 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)

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular

ST = unidade da federação do endereço físico do titular do certificado

L = cidade do endereço físico do titular

Business Category (OID 2.5.4.15) = tipo de categoria comercial, devendo conter: "Private Organization" ou "Government Entity" ou "Business Entity" ou "NonCommercial Entity"

SERIALNUMBER (OID 2.5.4.5) = CPF ou CNPJ, conforme o tipo de pessoa
Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR

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 IMPRENSA OFICIAL SSL são as seguintes:

- Não são admitidos sinais de acentuação, trema ou cedilhas;
- Os acentos devem ser substituídos pelo caractere não acentuado;
- O "ç" deve ser substituído pelo caractere 'c';
- Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
branco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(28
)	29
*	2A
+	2B

,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (OBJECT IDENTIFIER) DE POLÍTICA DE CERTIFICADO

O OID desta PC é: 2.16.76.1.2.4.42.

Todo certificado emitido segundo essa PC, PC A4 AC IMPRENSA OFICIAL SSL, contém o valor desse OID presente na extensão Certificate Policies.

7.1.7 USO DA EXTENSÃO "POLICY CONSTRAINTS"

Não se aplica.

7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Os campos policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC IMPRENSA OFICIAL SSL.

https://certificadodigital.imprensaoficial.com.br/media/files/ac_imprensa_oficial_ssl_dpc_v2_0.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 (S) DE VERSÃO

As LCR geradas pela AC IMPRENSA OFICIAL SSL 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 IMPRENSA OFICIAL SSL e sua criticidade.

7.2.2.2. As LCR da AC IMPRENSA OFICIAL SSL 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 que assina a LCR;
- b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC que assina a LCR.

A AC IMPRENSA OFICIAL SSL define como obrigatória a seguinte extensão para suas LCRs:

- a) "Authority Information Access", não crítica: contém o endereço web onde se poderá obter a cadeia de certificação
<http://certificadodigital.imprensaoficial.com.br/repositorio/ac/imespsl>

7.3. PERFIL DE OCSP

7.3.1. NÚMERO (S) DE VERSÃO

Serviços de respostas OCSP implementam a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. EXTENSÕES DE OCSP

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 IMPRENSA OFICIAL 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

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. RESPONSABILIDADES 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 informações 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. 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 nesta PC é submetida à aprovação da AC Raiz.

9.12.2. MECANISMO DE NOTIFICAÇÃO E PERÍODOS

Mudança nesta PC será publicado no site da AC IMPRENSA OFICIAL SSL.

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 IMPRENSA OFICIAL SSL e AR vinculadas. 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, durante o processo de credenciamento da AC IMPRENSA OFICIAL 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, foi verificada a compatibilidade entre a PC e a DPC da AC IMPRENSA OFICIAL 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 DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12
	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP 04

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](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 DA ICP-BRASIL	DOC-ICP-01.01
[2]	ATRIBUIÇÃO DA OID NA ICP-BRASIL	DOC-ICP-04.01