

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

**POLÍTICA DE CERTIFICADO DE ASSINATURA DIGITAL
== TIPO A3 ==**

VERSÃO 1.0 – 15/12/2016

HISTÓRICO DE VERSÕES

<i>Data</i>	<i>Versão</i>	<i>Observações</i>
15/12/2016	1.0	Redação Inicial

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.....	9
1.1.	Visão Geral.....	9
1.2.	Identificação.....	9
1.3.	Comunidade e Aplicabilidade.....	9
1.3.1.	Autoridades Certificadoras.....	9
1.3.2.	Autoridades de Registro.....	9
1.3.3.	Prestador de Serviço de Suporte.....	10
1.3.4.	Titulares de Certificado.....	10
1.3.5.	Aplicabilidade.....	10
1.4.	Dados de Contato.....	11
2.	Disposições Gerais.....	12
2.1.	Obrigações e Direitos.....	12
2.1.1.	Obrigações da AC Imprensa Oficial SSL.....	12
2.1.2.	Obrigações das AR.....	12
2.1.3.	Obrigações dos Titulares do Certificado.....	12
2.1.4.	Direitos da Terceira Parte (Relying Party).....	12
2.1.5.	Obrigações do Repositório.....	12
2.2.	Responsabilidades.....	12
2.2.1.	Responsabilidades da AC Imprensa Oficial SSL.....	12
2.2.2.	Responsabilidades das AR.....	12
2.3.	Responsabilidade Financeira.....	12
2.3.1.	Indenizações devidas pela terceira parte (Relying Party).....	12
2.3.2.	Relações Fiduciárias.....	12
2.3.3.	Processos Administrativos.....	12
2.4.	Interpretação e Execução.....	12
2.4.1.	Legislação.....	12
2.4.2.	Forma de interpretação e notificação.....	12
2.4.3.	Procedimentos de solução de disputa.....	12
2.5.	Tarifas de Serviço.....	13
2.5.1.	Tarifas de emissão e renovação de certificados.....	13
2.5.2.	Tarifas de acesso ao certificado.....	13
2.5.3.	Tarifas de revogação ou de acesso à informação de status.....	13
2.5.4.	Tarifas para outros serviços.....	13
2.5.5.	Política de reembolso.....	13
2.6.	Publicação e Repositório.....	13
2.6.1.	Publicação de informação da AC.....	13
2.6.2.	Frequência de publicação.....	13

2.6.3.	Controles de acesso	13
2.6.4.	Repositórios.....	13
2.7.	Auditoria e Fiscalização	13
2.8.	Sigilo	13
2.8.1.	Tipos de informações sigilosas	13
2.8.2.	Tipos de informações não-sigilosas	13
2.8.3.	Divulgação de informação de revogação ou suspensão de certificado	13
2.8.4.	Quebra de sigilo por motivos legais	13
2.8.5.	Informações a terceiros	13
2.8.6.	Divulgação por solicitação do Titular	13
2.8.7.	Outras circunstâncias de divulgação de informação	13
2.9.	Direitos de Propriedade Intelectual.....	13
3.	Identificação e Autenticação.....	14
3.1.	Registro Inicial.....	14
3.1.1.	Disposições Gerais	14
3.1.2.	Tipos de nomes.....	14
3.1.3.	Necessidade de nomes significativos.....	14
3.1.4.	Regras para interpretação de vários tipos de nomes	14
3.1.5.	Unicidade de nomes.....	14
3.1.6.	Procedimento para resolver disputa de nomes.....	14
3.1.7.	Reconhecimento, autenticação e papel de marcas registradas	14
3.1.8.	Método para comprovar a posse de chave privada	14
3.1.9.	Autenticação da identidade do indivíduo	14
3.1.10.	Autenticação da identidade de uma organização.....	14
3.1.11.	Autenticação da identidade de um equipamento ou aplicação.....	14
3.2.	Geração de novo par de chaves antes da expiração do atual.....	14
3.3.	Geração de novo par de chaves após revogação	14
3.4.	Solicitação de Revogação	14
4.	Requisitos Operacionais.....	15
4.1.	Solicitação de Certificado	15
4.2.	Emissão de Certificado	15
4.3.	Aceitação de Certificado	15
4.4.	Suspensão e Revogação de Certificado	15
4.4.1.	Circunstâncias para revogação	15
4.4.2.	Quem pode solicitar revogação	15
4.4.3.	Procedimento para solicitação de revogação	15
4.4.4.	Prazo para solicitação de revogação.....	15
4.4.5.	Circunstâncias para suspensão	15

4.4.6.	Quem pode solicitar suspensão	15
4.4.7.	Procedimento para solicitação de suspensão	15
4.4.8.	Limites no período de suspensão	15
4.4.9.	Frequência de emissão de LCR.....	15
4.4.10.	Requisitos para verificação de LCR	15
4.4.11.	Disponibilidade para revogação ou verificação de status on-line	15
4.4.12.	Requisitos para verificação de revogação on-line	15
4.4.13.	Outras formas disponíveis para divulgação de revogação	15
4.4.14.	Requisitos para verificação de outras formas de divulgação de revogação 15	
4.4.15.	Requisitos especiais para o caso de comprometimento de chave	15
4.5.	Procedimentos de Auditoria de Segurança	16
4.5.1.	Tipos de eventos registrados.....	16
4.5.2.	Frequência de auditoria de registros (logs)	16
4.5.3.	Período de retenção para registros (logs) de auditoria.....	16
4.5.4.	Proteção de registro (log) de auditoria	16
4.5.5.	Procedimentos para cópia de segurança (backup) de registro (log) de auditoria 16	
4.5.6.	Sistema de coleta de dados de auditoria	16
4.5.7.	Notificação de agentes causadores de eventos	16
4.5.8.	Avaliações de vulnerabilidade	16
4.6.	Arquivamento de Registros.....	16
4.6.1.	Tipos de registros arquivados.....	16
4.6.2.	Período de retenção para arquivo	16
4.6.3.	Proteção de arquivo	16
4.6.4.	Procedimentos para cópia de segurança (backup) de arquivo.....	16
4.6.5.	Requisitos para datação (time-stamping) de registros	16
4.6.6.	Sistema de coleta de dados de arquivo	16
4.6.7.	Procedimentos para obter e verificar informação de arquivo	16
4.7.	Troca de chave.....	16
4.8.	Comprometimento e Recuperação de Desastre	16
4.8.1.	Recursos computacionais, software, e dados corrompidos.....	16
4.8.2.	Certificado de entidade é revogado	16
4.8.3.	Chave de entidade é comprometida	16
4.8.4.	Segurança dos recursos após desastre natural ou de outra natureza	16
4.8.5.	Atividades das Autoridades de Registro.....	16
4.9.	Extinção dos serviços de AC, AR ou PSS.....	16
5.	Controles de Segurança Física, Procedimental e de Pessoal	17
5.1.	Controles Físicos	17

5.1.1.	Construção e localização das instalações.....	17
5.1.2.	Acesso físico	17
5.1.3.	Energia e ar condicionado	17
5.1.4.	Exposição à água	17
5.1.5.	Prevenção e proteção contra incêndio.....	17
5.1.6.	Armazenamento de mídia	17
5.1.7.	Destruição de lixo	17
5.1.8.	Instalações de segurança (backup) externas (off-site).....	17
5.2.	Controles Procedimentais.....	17
5.2.1.	Perfis qualificados	17
5.2.2.	Número de pessoas necessário por tarefa	17
5.2.3.	Identificação e autenticação para cada perfil.....	17
5.3.	Controles de Pessoal.....	17
5.3.1.	Antecedentes, qualificação, experiência e requisitos de idoneidade.....	17
5.3.2.	Procedimentos de verificação de antecedentes.....	17
5.3.3.	Requisitos de treinamento.....	17
5.3.4.	Frequência e requisitos para reciclagem técnica.....	17
5.3.5.	Frequência e sequência de rodízio de cargos.....	17
5.3.6.	Sanções para ações não autorizadas.....	17
5.3.7.	Requisitos para contratação de pessoal.....	17
5.3.8.	Documentação fornecida ao pessoal.....	17
6.	Controles Técnicos de Segurança.....	18
6.1.	Geração e Instalação do Par de Chaves	18
6.1.1.	Geração do par de chaves	18
6.1.2.	Entrega da chave privada à entidade titular do certificado	19
6.1.3.	Entrega da chave pública para emissor de certificado	19
6.1.4.	Disponibilização de chave pública da AC para usuários.....	19
6.1.5.	Tamanhos de chave	19
6.1.6.	Geração de parâmetros de chaves assimétricas	19
6.1.7.	Verificação da qualidade dos parâmetros.....	19
6.1.8.	Geração de chave por hardware ou software.....	19
6.1.9.	Propósitos de uso de chave (conforme o campo “key usage” na X.509v3) 19	
6.2.	Proteção da Chave Privada	20
6.2.1.	Padrões para módulo criptográfico	20
6.2.2.	Controle “n de m” para chave privada	20
6.2.3.	Recuperação (escrow) de chave privada	20
6.2.4.	Cópia de segurança (backup) de chave privada	20
6.2.5.	Arquivamento de chave privada.....	20

6.2.6.	Inserção de chave privada em módulo criptográfico	20
6.2.7.	Método de ativação de chave privada.....	21
6.2.8.	Método de desativação de chave privada.....	21
6.2.9.	Método de destruição de chave privada.....	21
6.3.	Outros Aspectos do Gerenciamento do Par de Chaves	21
6.3.1.	Arquivamento de chave pública.....	21
6.3.2.	Períodos de uso para as chaves pública e privada	21
6.4.	Dados de Ativação	21
6.4.1.	Geração e instalação dos dados de ativação.....	21
6.4.2.	Proteção dos dados de ativação.....	21
6.4.3.	Outros aspectos dos dados de ativação.....	21
6.5.	Controles de Segurança Computacional	22
6.5.1.	Requisitos técnicos específicos de segurança computacional.....	22
6.5.2.	Classificação da segurança computacional.....	22
6.6.	Controles Técnicos do Ciclo de Vida	22
6.6.1.	Controles de desenvolvimento de sistema.....	22
6.6.2.	Controles de gerenciamento de segurança	22
6.6.3.	Classificações de segurança de ciclo de vida.....	22
6.7.	Controles de Segurança de Rede	22
6.8.	Controles de Engenharia do Módulo Criptográfico.....	22
7.	Perfis de Certificado e LCR	23
7.1.	Perfil do Certificado	23
7.1.1.	Número de versão.....	23
7.1.2.	Extensões de certificado	23
7.1.3.	Identificadores de algoritmo.....	26
7.1.4.	Formatos de nome.....	26
7.1.5.	Restrições de nome	26
7.1.6.	OID (Object Identifier) de Política de Certificado	27
7.1.7.	Uso da extensão "Policy Constraints"	27
7.1.8.	Sintaxe e semântica dos qualificadores de política	27
7.1.9.	Semântica de processamento para extensões críticas.....	27
7.2.	Perfil de LCR.....	27
7.2.1.	Número(s) de versão	28
7.2.2.	Extensões de LCR e de suas entradas.....	28
8.	Administração de Especificação	29
8.1.	Procedimentos de mudança de especificação.....	29
8.2.	Políticas de publicação e notificação	29
8.3.	Procedimentos de aprovação.....	29

9. Documentos Referenciados 30

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 A3 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 A3.

1.1.4. Não se aplica.

1.1.5. Não se aplica.

1.1.6. Não se aplica.

1.1.7. Não se aplica.

1.2. IDENTIFICAÇÃO

1.2.1 Esta PC é designada de “Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora Imprensa Oficial SSL” e referida como “PC A3 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 A3. O OID (object identifier) desta PC é 2.16.76.1.2.3.209.

1.2.2. Não se aplica.

1.3. COMUNIDADE E APLICABILIDADE

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).

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://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/>):

- a) relação de todas as AR credenciadas, com informações sobre as PC que implementam.

- b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar.
- c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades.
- d) relação de AR que tenham se descredenciado da cadeia da AC Imprensa Oficial SSL, com respectiva data do descredenciamento.
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades.
- f) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2. A AC Imprensa Oficial SSL mantém as informações acima sempre atualizadas.

1.3.3. PRESTADOR DE SERVIÇO DE SUPORTE

1.3.3.1. A relação de todos os Prestadores de Serviço de Suporte – PSS vinculados diretamente a AC Imprensa Oficial SSL e/ou por intermédio de suas AR é publicada em serviço de diretório e/ou em página web da AC Imprensa Oficial SSL (<http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/http://www.digitaltrust.com.br/repositorio/rfb-v1/>).

1.3.3.2. PSS são entidades utilizadas pela AC e/ou suas AR para desempenhar atividade descrita nesta PC e se classificam em três categorias, conforme o tipo de atividade prestada:

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

1.3.3.3. A AC Imprensa Oficial SSL mantém as informações acima sempre atualizadas.

1.3.4. TITULARES DE CERTIFICADO

Os titulares de certificado de assinatura do Tipo A3 podem ser pessoas físicas ou jurídicas, observando o disposto nos itens 1.3.4, 3.1.9, 3.1.10 e 3.1.11 da DPC.

1.3.5. APLICABILIDADE

1.3.5.1. 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.

1.3.5.2. 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.

1.3.5.3. 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.

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

- Acesso a aplicações disponibilizadas pela Receita Federal do Brasil, ou por qualquer outro órgão da Administração Pública Direta ou Indireta, que aceitem este certificado;
- Confirmação de identidade na Web;
- Transações eletrônicas e transações on-line;
- Redes privadas virtuais (VPN);
- Cifração de chaves de sessão.

1.3.5.5. Não se aplica.

1.3.5.6. Não se aplica.

1.4. DADOS DE CONTATO

Imprensa Oficial do Estado SA IMESP.
Rua da Mooca, 1921 – Mooca – São Paulo, SP
Telefone: (55 11) 0800 0123401
Fax: (55 11) 2799 9887
Nome: João Paulo Foini
Telefone: (55 11) 2799 9800
Email: certificacao@imprensaoficial.com.br

2. DISPOSIÇÕES GERAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SSL.

2.1. OBRIGAÇÕES E DIREITOS

2.1.1. OBRIGAÇÕES DA AC IMPRENSA OFICIAL SSL

2.1.2. OBRIGAÇÕES DAS AR

2.1.3. OBRIGAÇÕES DOS TITULARES DO CERTIFICADO

2.1.4. DIREITOS DA TERCEIRA PARTE (RELYING PARTY)

2.1.5. OBRIGAÇÕES DO REPOSITÓRIO

2.2. RESPONSABILIDADES

2.2.1. RESPONSABILIDADES DA AC IMPRENSA OFICIAL SSL

2.2.2. RESPONSABILIDADES DAS AR

2.3. RESPONSABILIDADE FINANCEIRA

2.3.1. INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE (RELYING PARTY)

2.3.2. RELAÇÕES FIDUCIÁRIAS

2.3.3. PROCESSOS ADMINISTRATIVOS

2.4. INTERPRETAÇÃO E EXECUÇÃO

2.4.1. LEGISLAÇÃO

2.4.2. FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO

2.4.3. PROCEDIMENTOS DE SOLUÇÃO DE DISPUTA

2.5. TARIFAS DE SERVIÇO

- 2.5.1. TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS**
- 2.5.2. TARIFAS DE ACESSO AO CERTIFICADO**
- 2.5.3. TARIFAS DE REVOGAÇÃO OU DE ACESSO À INFORMAÇÃO DE STATUS**
- 2.5.4. TARIFAS PARA OUTROS SERVIÇOS**
- 2.5.5. POLÍTICA DE REEMBOLSO**

2.6. PUBLICAÇÃO E REPOSITÓRIO

- 2.6.1. PUBLICAÇÃO DE INFORMAÇÃO DA AC**
- 2.6.2. FREQUÊNCIA DE PUBLICAÇÃO**
- 2.6.3. CONTROLES DE ACESSO**
- 2.6.4. REPOSITÓRIOS**

2.7. AUDITORIA E FISCALIZAÇÃO

2.8. SIGILO

- 2.8.1. TIPOS DE INFORMAÇÕES SIGILOSAS**
- 2.8.2. TIPOS DE INFORMAÇÕES NÃO-SIGILOSAS**
- 2.8.3. DIVULGAÇÃO DE INFORMAÇÃO DE REVOGAÇÃO OU SUSPENSÃO DE CERTIFICADO**
- 2.8.4. QUEBRA DE SIGILO POR MOTIVOS LEGAIS**
- 2.8.5. INFORMAÇÕES A TERCEIROS**
- 2.8.6. DIVULGAÇÃO POR SOLICITAÇÃO DO TITULAR**
- 2.8.7. OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO**

2.9. DIREITOS DE PROPRIEDADE INTELECTUAL

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SSL.

3.1. REGISTRO INICIAL

3.1.1. DISPOSIÇÕES GERAIS

3.1.2. TIPOS DE NOMES

3.1.3. NECESSIDADE DE NOMES SIGNIFICATIVOS

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

3.1.8. MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA

3.1.9. AUTENTICAÇÃO DA IDENTIDADE DO INDIVÍDUO

3.1.9.1. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

3.1.9.2. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

3.1.10. AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

3.1.10.1. DISPOSIÇÕES GERAIS

3.1.10.2. DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

3.1.10.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO

3.1.11. AUTENTICAÇÃO DA IDENTIDADE DE UM EQUIPAMENTO OU APLICAÇÃO

3.1.11.1. DISPOSIÇÕES GERAIS

3.1.11.2. PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO OU APLICAÇÃO

3.1.11.3. INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO OU APLICAÇÃO

3.2. GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.3. GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO

3.4. SOLICITAÇÃO DE REVOGAÇÃO

4. REQUISITOS OPERACIONAIS

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SSL.

4.1. SOLICITAÇÃO DE CERTIFICADO

4.2. EMISSÃO DE CERTIFICADO

4.3. ACEITAÇÃO DE CERTIFICADO

4.4. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1. CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.4.2. QUEM PODE SOLICITAR REVOGAÇÃO

4.4.3. PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.4. PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.5. CIRCUNSTÂNCIAS PARA SUSPENSÃO

4.4.6. QUEM PODE SOLICITAR SUSPENSÃO

4.4.7. PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO

4.4.8. LIMITES NO PERÍODO DE SUSPENSÃO

4.4.9. FREQUÊNCIA DE EMISSÃO DE LCR

4.4.10. REQUISITOS PARA VERIFICAÇÃO DE LCR

4.4.11. DISPONIBILIDADE PARA REVOGAÇÃO OU VERIFICAÇÃO DE STATUS ON-LINE

4.4.12. REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

4.4.13. OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

4.4.14. REQUISITOS PARA VERIFICAÇÃO DE OUTRAS FORMAS DE DIVULGAÇÃO DE REVOGAÇÃO

4.4.15. REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.5. PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

- 4.5.1. TIPOS DE EVENTOS REGISTRADOS**
- 4.5.2. FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS)**
- 4.5.3. PERÍODO DE RETENÇÃO PARA REGISTROS (LOGS) DE AUDITORIA**
- 4.5.4. PROTEÇÃO DE REGISTRO (LOG) DE AUDITORIA**
- 4.5.5. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO (LOG) DE AUDITORIA**
- 4.5.6. SISTEMA DE COLETA DE DADOS DE AUDITORIA**
- 4.5.7. NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS**
- 4.5.8. AVALIAÇÕES DE VULNERABILIDADE**

4.6. ARQUIVAMENTO DE REGISTROS

- 4.6.1. TIPOS DE REGISTROS ARQUIVADOS**
- 4.6.2. PERÍODO DE RETENÇÃO PARA ARQUIVO**
- 4.6.3. PROTEÇÃO DE ARQUIVO**
- 4.6.4. PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE ARQUIVO**
- 4.6.5. REQUISITOS PARA DATAÇÃO (TIME-STAMPING) DE REGISTROS**
- 4.6.6. SISTEMA DE COLETA DE DADOS DE ARQUIVO**
- 4.6.7. PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO**

4.7. TROCA DE CHAVE

4.8. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

- 4.8.1. RECURSOS COMPUTACIONAIS, SOFTWARE, E DADOS CORROMPIDOS**
- 4.8.2. CERTIFICADO DE ENTIDADE É REVOGADO**
- 4.8.3. CHAVE DE ENTIDADE É COMPROMETIDA**
- 4.8.4. SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA**
- 4.8.5. ATIVIDADES DAS AUTORIDADES DE REGISTRO**

4.9. EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são referidos os itens correspondentes da DPC da AC Imprensa Oficial SSL.

5.1. CONTROLES FÍSICOS

- 5.1.1. CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES**
- 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)**

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**

5.3. 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**

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.

6.1.1.2. A geração do par de chaves criptográficas ocorre utilizando um cartão inteligente, token criptográfico, ou outro devidamente homologado.

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].

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 chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- 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;
- 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. O tipo de certificado emitido pela AC Imprensa Oficial SSL descrito nesta PC é o A3.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A3	Cartão Inteligente ou Token, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou hardware criptográfico homologado junto à ICP-Brasil.

6.1.2. ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR DO CERTIFICADO

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. DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC PARA USUÁRIOS

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://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/ACIMESPSSL.p7b>.

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 de 2048 bits.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 da ICP-Brasil está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1].

6.1.6. GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão FIPS (Federal Information Processing Standards) 140-1 ou equivalente estabelecido pelo CG da ICP-Brasil.

6.1.7. VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

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

6.1.8. GERAÇÃO DE CHAVE POR HARDWARE OU SOFTWARE

A geração das chaves criptográficas do Certificado Tipo A3 desta PC, é realizada por hardware criptográfico aprovado pelo CG da ICP-Brasil.

6.1.9. 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

6.2.1. PADRÕES PARA MÓDULO CRIPTOGRÁFICO

Não se aplica

6.2.2. CONTROLE “N DE M” PARA CHAVE PRIVADA

Não se aplica.

6.2.3. RECUPERAÇÃO (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

Não se aplica.

6.2.7. MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

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

6.2.8. MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

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

6.2.9. 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 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 A3 é de 5 (cinco) anos.

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.

O equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados possui conexão com o dispositivo de mídia inteligente e o respectivo driver instalado. A mídia inteligente possui processador criptográfico com capacidade de geração interna das chaves.

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. CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA

Não se aplica.

6.7. CONTROLES DE SEGURANÇA DE REDE

Não se aplica.

6.8. CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado deverá estar em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7. PERFIS DE CERTIFICADO E LCR

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 campo policyIdentifier contém o OID desta PC: 2.16.76.1.2.3.209;
 - O campo policyQualifiers contém o endereço Web da DPC da AC que emite o certificado: <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/>
- d) "CRL Distribution Points", não crítica: contém os endereços Web onde se obtém a LCR correspondente:
 - <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/ACIMESPSSL.crl>
 - <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://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/ACIMESPSSL.p7b>
- f) "Extended Key Usage", não crítica, contém:
 - para certificados de assinatura de OCSP: somente o propósito "OCSPSigning" (OID 1.3.6.1.5.5.7.3.9) deve estar ativado;
 - outros certificados: no mínimo o propósito "server authentication" (OID 1.3.6.1.5.5.7.3.1) e podendo conter o valor "client authentication" (OID 1.3.6.1.5.5.7.3.2), podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pela AC, em suas PC.
- g) "Basic Constraints", não crítica:
 - Subject Type = End Entity; e
 - Path Length Constraint=None

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) Para certificado de pessoa física (e-CPF):
 - a.1) 3 (três) campos otherName, obrigatórios, contendo:
 - i. OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;
 - ii. OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado;
 - iii. OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.
 - a.2) campo otherName, não obrigatório, contendo:
 - i. OID = 2.16.76.1.4.n e conteúdo = de tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente. A AC Raiz regulamenta a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.
- b) Para certificado de pessoa Jurídica (e-CNPJ):
 - b.1) 4 (quatro) campos otherName, contendo:
 - i. OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social – NIS (PIS, PASEP ou CI) do responsável; nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.
 - ii. OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pela Pessoa Jurídica.
 - iii. OID = 2.16.76.1.3.3 e conteúdo = Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.
 - iv. OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.
- 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.

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. No caso de múltiplas habilitações profissionais, são inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas.
- 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) Para os campos `OtherName`, com exceção do UPN, 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.

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. Não se aplica.

7.1.3. IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Imprensa Oficial SSL são assinados utilizando o algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) conforme o padrão PKCS#1.

7.1.4. FORMATOS DE NOME

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

C = BR

ST = <Sigla da Unidade de Federação>

L = <Cidade>

O = ICP-Brasil

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

OU = <Identificação da AR>

CN = <Nome do titular>

Onde:

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

O identificador CN contém o URL correspondente ou o nome da aplicação.

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.

7.1.5. 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: 2.16.76.1.2.3.209

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. (<http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/>)

7.1.9. SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

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 criticalidade.

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;
- c) "Authority Information Access", não crítica: contém o endereço web onde se poderá obter a cadeia de certificação. (<http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/ACIMESPSSL.p7b>).

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração a esta PC implica a adoção de nova versão e está sujeita à autorização da AC Raiz.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

Esta PC é de consulta pública, e está disponibilizada no endereço Web: <http://io-com-icpbr.imprensaoficial.com.br/repositorio/IMESPSSL/>

8.3. PROCEDIMENTOS DE APROVAÇÃO

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC Imprensa Oficial SSL, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

9. DOCUMENTOS REFERENCIADOS

9.1. Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

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

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01