CERTIFICADOS DIGITAIS-AUTORIDADE DE REGISTRO SERPRO

# Política de Certificação
# da
# Autoridade Certificadora
# INFOCOMEX SE-S

**Garantia da origem e integridade**

(PC AC INFOCOMEX SE-S)

Versão 1.0 de Setembro de 2026

# SUMÁRIO

CONTROLE DE ALTERAÇÕES....3
1. INTRODUÇÃO....4
1.1. Visão Geral....4
1.2. Nome do documento e Identificação....4
1.3. Participantes da ICP-Brasil....4
1.4. Usabilidade do Certificado....5
1.5. Política de Administração....6
1.6. Definições e Acrônimos....7
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO....8
3. IDENTIFICAÇÃO E AUTENTICAÇÃO....8
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO....9
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES....12
6. CONTROLES TÉCNICOS DE SEGURANÇA....14
6.1. Geração e Instalação do Par de Chaves....14
6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico....16
6.3 Outros Aspectos do Gerenciamento do Par de Chaves....17
6.4. Dados de Ativação....18
6.5. Controles de Segurança Computacional....18
6.6. Controles Técnicos do Ciclo de Vida....18
6.7. Controles de Segurança de Rede....19
6.8. Carimbo do Tempo....19
7. PERFIS DE CERTIFICADO, LCR E OCSP....19
7.1. Perfil do Certificado....19
7.2. Perfil de LCR....22
7.3. Perfil de OCSP....23
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES....23
9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS....23
10. DOCUMENTOS REFERENCIADOS....26
11. REFERÊNCIAS BIBLIOGRÁFICAS....27

# CONTROLE DE ALTERAÇÕES

| Versão | Data | Responsável | Motivo | Descrição |
|---|---|---|---|---|
| 1.0 | Setembro/2026 | Fernando Morgado<br>Lucia Castelli | Versão Inicial | Versão inicial compatívelcom a versão 8.3 do DOC-ICP-04(PC)-https://www.iti.gov.br |
| 1.0 | Setembro/2026 | Alice Vasconcellos | Aprovação | |

# 1. INTRODUÇÃO

## 1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos a serem obrigatoriamente observados pela Autoridade Certificadora da Empresa INFOCOMEX INFORMATICA LTDA credenciada como AC INFOCOMEX, integrante da infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado - PC.

1.1.2. A PC AC INFOCOMEX SE-S, elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO na ICP-BRASIL[3].

1.1.3. A estrutura desta PC está baseada na RFC 3647.

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

1.1.5. O tipo de certificado emitido, sob esta política de certificado, é o certificado digital de selo eletrônico em software - SE-S..

1.1.6. Não se aplica.

1.1.7. Certificados do tipo SE-S são certificados de selo eletrônico em software, e devem ser emitidos apenas para pessoas jurídicas.

1.1.8. Não se aplica.

1.1.9. Não se aplica.

1.1.10. Não se aplica.

1.1.11. Não se aplica.

1.1.12. Não se aplica.

## 1.2. Nome do documento e Identificação

1.2.1. Política de Certificado Digital de selo eletrônico, SE-S , da AC INFOCOMEX, tendo o seguinte OID:

| PC AC INFOCOMEX SE-S | OID 2.16.76.1.2.201.27 |
|---|---|

1.2.2. No âmbito da ICP-Brasil, o OID desta PC foi atribuído na conclusão do processo de credenciamento da AC INFOCOMEX.

## 1.3. Participantes da ICP-Brasil

### 1.3.1. Autoridades Certificadoras

1.3.1.1. A Autoridade Certificadora INFOCOMEX AC INFOCOMEX integra a infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora do SERPRO

(AC SERPRO) e da Autoridade Certificadora Raiz Brasileira, cuja PC é implementada nesse documento.

1.3.1.2. A DPC dessa AC encontra-se publicada em sua página *Web* no seguinte endereço: http://repositorio.serpro.gov.br/docs/dpcacinfocomex.pdf.

### 1.3.2. Autoridades de Registro

1.3.2.1. O endereço da página *web* (*URL*) da AC INFOCOMEX é https://certificados.serpro.gov.br/acinfocomex onde estão publicados os dados abaixo referentes as Autoridades de Registro, responsáveis pelos processos de recebimento, identificação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

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

b) relação de AR que tenham sido descredenciadas da cadeia da AC, com a respectiva data do descredenciamento;

### 1.3.3. Titulares do Certificado

Os Titulares de Certificados desta política de certificado, são pessoas jurídicas, autorizadas por AR vinculada a receber um certificado digital emitido pela AC para sua própria utilização.

### 1.3.4. Partes Confiáveis

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

### 1.3.5. Outros Participantes

A AC utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS, Prestador de Serviço Biométrico – PSBio e Prestador de Serviço de Confiança - PSC conforme disponibilizado no endereço: https://certificados.serpro.gov.br/acinfocomex .

## 1.4. Usabilidade do Certificado

### 1.4.1. Uso apropriado do certificado

1.4.1.1. Os certificados de tipo Selo Eletrônico de Software(SE-S), são utilizados para garantir origem e integridade de um documento eletrônico, servindo de prova da emissão do documento por uma pessoa jurídica.

1.4.1.2. As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo, contemplado pela ICP-Brasil, aceitam qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3. As aplicações para o certificado definido nesta PC, levam em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado.

1.4.1.4. Não se aplica.

1.4.1.5. Certificados do tipo SE-S serão utilizados para garantir origem e integridade deum documento eletrônico, servindo de prova da emissão do documento por uma pessoa jurídica

1.4.1.6. Não se aplica.

1.4.1.7. Não se aplica.

1.4.1.8. Não se aplica.

1.4.1.9. Não se aplica.

### 1.4.2. Uso proibitivo do certificado

1.4.2.1 Não aplicado.

1.4.2.2 É proibido o uso do certificado de selo eletrônico para assinatura digital com o propósito de manifestação de vontade.

1.4.2.3 Não aplicado.

## 1.5. Política de Administração

Esta PC é administrada pela própria AC INFOCOMEX.

### 1.5.1. Organização administrativa do documento

Autoridade Certificadora INFOCOMEX – AC INFOCOMEX.

### 1.5.2. Contatos

**Administrativo:**

Nome: LUCIANO TEIXEIRA DE ABREU

Endereço: Av Coronel Marcos Konder, 1313 – Sala 07 – Centro – Itajaí / SC

CEP: 88.301-904

E-mail: luciano@infocomex.com.br

Telefone: (47) 3249-1347

**Suporte:**

Nome: Central de Serviços SERPRO
Página Web: https://atendimento.serpro.gov.br/certificacaodigital
E-mail: css.serpro@serpro.gov.br
Telefone: 0800 7282323

### 1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: LUCIANO TEIXEIRA DE ABREU

Telefone: (47) 3249-1347

E-mail: luciano@infocomex.com.br

### 1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.

## 1.6. Definições e Acrônimos

| Sigla | Definição |
|---|---|
| AC | Autoridade Certificadora |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| AR | Autoridades de Registro |
| CEI | Cadastro Específico do INSS |
| CG ICP-Brasil | Comitê Gestor da ICP-Brasil |
| CMM-SEI | Capability Maturity Model do Software Engineering Institute |
| CMVP | Cryptographic Module Validation Program |
| CN | Common Name |
| CNPJ | Cadastro Nacional de Pessoas Jurídicas |
| CPF | Cadastro de Pessoas Físicas |
| DN | Distinguished Name |
| DPC | Declaração de Práticas de Certificação |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IEC | International Electrotechnical Commission |
| ISO | International Organization for Standardization |
| ITU | International Telecommunications Union |
| LCR | Lista de Certificados Revogados |
| NBR | Norma Brasileira |
| NIS | Número de Identificação Social |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OU | Organization Unit |
| PASEP | Programa de Formação do Patrimônio do Servidor Público |
| PC | Políticas de Certificado |
| PCN | Plano de Continuidade de Negócio |
| PIS | Programa de Integração Social |
| POP | Proof of Possession |
| PS | Política de Segurança |
| PSC | Prestador de Serviço de Confiança |
| PSS | Prestadores de Serviço de Suporte |
| RFC | Request For Comments |
| RG | Registro Geral |
| SSL | Secure Socket Layer |
| UF | Unidade de Federação |
| URL | Uniform Resource Locator |

# 2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão descritos na DPC da AC.

### 2.1. Repositórios

### 2.2. Publicação de informações dos certificados

### 2.3. Tempo ou Frequência de Publicação

### 2.4. Controle de Acesso aos Repositórios

# 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão descritos na DPC da AC.

### 3.1. Nomeação

### 3.1.1. Tipos de nomes

### 3.1.2. Necessidade dos nomes serem significativos

### 3.1.3. Anonimato ou Pseudônimo dos Titulares do Certificado

### 3.1.4. Regras para interpretação de vários tipos de nomes

### 3.1.5. Unicidade de nomes

### 3.1.6. Procedimento para resolver disputa de nomes

### 3.1.7. Reconhecimento, autenticação e papel de marcas registradas

### 3.2. Validação inicial de identidade

### 3.2.1. Método para comprovar a posse de chave privada

### 3.2.2. Autenticação da identificação da organização

### 3.2.3. Autenticação da identidade de equipamento ou aplicação

Item 3.2.7. da DPC.

### 3.2.4. Autenticação da identidade de um indivíduo

Item 3.2.3. da DPC.

### 3.2.5. Informações não verificadas do titular do certificado

Item 3.2.4. da DPC.

### 3.2.6. Validação das autoridades

Item 3.2.5. da DPC.

### 3.2.7. Critérios para interoperação

Iem 3.2.6. da DPC.

### 3.3. Identificação e autenticação para pedidos de novas chaves

### 3.3.1. Identificação e autenticação para rotina de novas chaves antes da expiração

### 3.3.2. Identificação e autenticação para novas chaves após a revogação ou expiração do certificado

### 3.4. Identificação e Autenticação para solicitação de revogação

## 4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Os itens seguintes estão descritos na DPC da AC.

### 4.1. Solicitação do certificado

### 4.1.1. Quem pode submeter uma solicitação de certificado

### 4.1.2. Processo de registro e responsabilidades

### 4.2. Processamento de Solicitação de Certificado

### 4.2.1. Execução das funções de identificação e autenticação

### 4.2.2. Aprovação ou rejeição de pedidos de certificado

### 4.2.3. Tempo para processar a solicitação de certificado

### 4.3. Emissão de Certificado

### 4.3.1. Ações da AC durante a emissão de um certificado

### 4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

### 4.4. Aceitação de Certificado

### 4.4.1. Conduta sobre a aceitação do certificado

### 4.4.2. Publicação do certificado pela AC

### 4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades

### 4.5. Usabilidade do par de chaves e do certificado

### 4.5.1. Usabilidade da Chave privada e do certificado do titular

### 4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

### 4.6. Renovação de Certificados

### 4.6.1. Circunstâncias para renovação de certificados

### 4.6.2. Quem pode solicitar a renovação

### 4.6.3. Processamento de requisição para renovação de certificados

### 4.6.4. Notificação para nova emissão de certificado para o titular

### 4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

### 4.6.6. Publicação de uma renovação de um certificado pela AC

### 4.6.7. Notificação de emissão de certificado pela AC para outras entidades

### 4.7. Nova chave de certificado

### 4.7.1. Circunstâncias para nova chave de certificado

### 4.7.2. Quem pode requisitar a certificação de uma nova chave pública

### 4.7.3. Processamento de requisição de novas chaves de certificado

### 4.7.4. Notificação de emissão de novo certificado para o titular

### 4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

### 4.7.6. Publicação de uma nova chave certificada pela AC

### 4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

### 4.8. Modificação de certificado

### 4.8.1. Circunstâncias para modificação de certificado

### 4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

### 4.8.3. Processamento de requisição de modificação de certificado

### 4.8.4. Notificação de emissão de novo certificado para o titular

### 4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

### 4.8.6. Publicação de uma modificação de certificado pela AC

**4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades**

**4.9. Suspensão e Revogação de Certificado**

**4.9.1. Circunstâncias para revogação**

**4.9.2. Quem pode solicitar revogação**

**4.9.3. Procedimento para solicitação de revogação**

**4.9.4. Prazo para solicitação de revogação**

**4.9.5. Tempo em que a AC deve processar o pedido de revogação**

**4.9.6. Requisitos de verificação de revogação para as partes confiáveis**

**4.9.7. Frequência de emissão de LCR**

**4.9.8. Latência máxima para a LCR**

**4.9.9. Disponibilidade para revogação/verificação de status on-line**

**4.9.10. Requisitos para verificação de revogação on-line**

**4.9.11. Outras formas disponíveis para divulgação de revogação**

**4.9.12. Requisitos especiais para o caso de comprometimento de chave**

**4.9.13. Circunstâncias para suspensão**

**4.9.14. Quem pode solicitar suspensão**

**4.9.15. Procedimento para solicitação de suspensão**

**4.9.16. Limites no período de suspensão**

**4.10. Serviços de status de certificado**

**4.10.1. Características operacionais**

**4.10.2. Disponibilidade dos serviços**

**4.10.3. Funcionalidades operacionais**

**4.11. Encerramento de atividades**

**4.12. Custódia e recuperação de chave**

**4.12.1. Política e práticas de custódia e recuperação de chave**

### 4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

## 5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES

Os itens seguintes estão descritos na DPC da AC.

### 5.1. Controles físicos

### 5.1.1 Construção e localização das instalações de AC

### 5.1.2. Acesso físico

### 5.1.3. Energia e ar-condicionado

### 5.1.4. Exposição à água

### 5.1.5. Prevenção e proteção contra incêndio

### 5.1.6. Armazenamento de mídia

### 5.1.7. Destruição de lixo

### 5.1.8. Instalações de segurança (*backup*) externas (*off-site*) para AC

### 5.2. Controles Procedimentais

### 5.2.1. Perfis qualificados

### 5.2.2. Número de pessoas necessário por tarefa

### 5.2.3. Identificação e autenticação para cada perfil

### 5.2.4. Funções que requerem separação de deveres

### 5.3. Controles de Pessoal

### 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

### 5.3.2. Procedimentos de verificação de antecedentes

### 5.3.3. Requisitos de treinamento

### 5.3.4. Frequência e requisitos para reciclagem técnica

### 5.3.5. Frequência e sequência de rodízio de cargos

### 5.3.6. Sanções para ações não autorizadas

### 5.3.7. Requisitos para contratação de pessoal

**5.3.8. Documentação fornecida ao pessoal**

**5.4. Procedimentos de Log de Auditoria**

**5.4.1. Tipos de eventos registrados**

**5.4.2. Frequência de auditoria de registros**

**5.4.3. Período de retenção para registros de auditoria**

**5.4.4. Proteção de registros de auditoria**

**5.4.5. Procedimentos para cópia de segurança (*backup*) de registros de auditoria**

**5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)**

**5.4.7. Notificação de agentes causadores de eventos**

**5.4.8. Avaliações de vulnerabilidade**

**5.5. Arquivamento de Registros**

**5.5.1. Tipos de registros arquivados**

**5.5.2. Período de retenção para arquivo**

**5.5.3. Proteção de arquivo**

**5.5.4. Procedimentos de cópia de arquivo**

**5.5.5. Requisitos para datação de registros**

**5.5.6. Sistema de coleta de dados de arquivo (interno e externo)**

**5.5.7. Procedimentos para obter e verificar informação de arquivo**

**5.6. Troca de chave**

**5.7. Comprometimento e Recuperação de Desastre**

**5.7.1. Procedimentos gerenciamento de incidente e comprometimento**

**5.7.2. Recursos computacionais, software, e/ou dados corrompidos**

**5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade**

**5.7.4. Capacidade de continuidade de negócio após desastre**

**5.8. Extinção da AC**

# 6. CONTROLES TÉCNICOS DE SEGURANÇA

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

## 6.1. Geração e Instalação do Par de Chaves

### 6.1.1. Geração do par de chaves

6.1.1.1. Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1. Não se aplica.

6.1.1.1.2. Não se aplica.

6.1.1.2. As chaves criptográficas dos titulares de certificados observam os requisitos desta PC, bem como ser geradas e armazenadas em hardware ou mídia criptográficos homologados pela ICP-Brasil.

6.1.1.3. O algoritmo utilizado para as chaves criptográficas de titulares de certificados dessa AC é RSA com tamanho de chaves de 2048 bits.

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a tabela a seguir:

| Tipo de Certificado | Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos) |
|---|---|
| SE-S | Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima. |

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

6.1.1.6. A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;

b) a chave privada não pode, com uma segurança razoável, ser deduzida e ser protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

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

6.1.1.8. O armazenamento de chaves privadas de terceiros em hardware criptográfico só é realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em *HSM* de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

**Nota:** Não se aplica.

### 6.1.2. Entrega da chave privada à entidade titular

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

### 6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação.

### 6.1.4. Entrega de chave pública da AC às terceiras partes

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL[1];

b) Não se aplica;

c) Página *web* da AC, disponível no seguinte endereço https://certificados.serpro.gov.br/acinfocomex ; e

d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

### 6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC é de, no mínimo, 2048 (dois mil e quarenta e oito) bits.

6.1.5.2. Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1].

### 6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

Os parâmetros de geração e verificação de chaves assimétricas do usuário final adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

Os certificados emitidos pela AC têm no campo “Key usage” (**2.5.29.15**) ativado os bits *digitalSignature, nonRepudiation e keyEncipherment.*

Os certificados emitidos sob esta PC pela AC INFOCOMEX são apropriados ao uso apenas nas aplicações apresentadas a seguir:

a) Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação pessoal. Eles podem ser usados nas seguintes aplicações;

b) Confirmação de Identidade na web;

c) Correio eletrônico;

d) Transações online;

e) Redes privadas virtuais (VPN);

f) Transações eletrônicas; e

g) Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

## 6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Neste item são definidos os requisitos de proteção das chaves privadas de certificados emitidos segundo a PC.

### 6.2.1. Padrão e controle para módulo criptográfico

6.2.1.1. Não se aplica.

6.2.1.2. 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 se aplica.

### 6.2.4. Cópia de segurança (*backup*) de chave privada

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

6.2.4.2. A AC não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Não se aplica.

6.2.4.4. Não se aplica.

### 6.2.5. Arquivamento de chave privada

6.2.5.1. Não se aplica.

6.2.5.2. Não se aplica.

### 6.2.6. Inserção de chave privada em módulo criptográfico

As chaves privadas são inseridas nos módulos criptográficos de acordo com os procedimentos especificados pelos fornecedores dos módulos.

### 6.2.7. Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

### 6.2.8. Método de ativação de chave privada

A chave privada é ativada, mediante senha solicitada pelo hardware de proteção da chave privada. A senha é criada e mantida apenas pelo Titular do Certificado, sendo para seu uso e conhecimento exclusivo.

O Titular de certificado adota senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 3 (três) meses.

### 6.2.9. Método de desativação de chave privada

A desativação da chave privada ocorre no fechamento do "*browser*" utilizado para estabelecer uma conexão segura.

### 6.2.10. Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado é feita através de software disponibilizado pelo fabricante da mídia, que permite apagar todas as informações nela contida, utilizando para isso a senha de acesso do titular do certificado à mídia armazenadora.

## 6.3 Outros Aspectos do Gerenciamento do Par de Chaves

### 6.3.1. Arquivamento de chave pública

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCR emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

### 6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1. A chave privada da AC e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC é utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Item revogado pela Resolução 211/2025.

6.3.2.3. O período máximo de validade admitido para o tipo de certificado previsto nessa PC, é:

Certificados do tipo SE-S, previsto nesta PC, tem validade de até 1 ano.

6.3.2.4. Não se aplica.

6.3.2.5. Não se aplica.

## 6.4. Dados de Ativação

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

### 6.4.1. Geração e instalação dos dados de ativação

Não se aplica.

### 6.4.2. Proteção dos dados de ativação

Não se aplica.

### 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

Os pares de chaves criptográficas dos titulares de certificados observam os requisitos gerais desta PC, bem como ser geradas e armazenadas em hardware ou mídia criptográficos homologados pela ICP-Brasil.
Nos equipamentos onde são gerados os pares de chaves criptográficas dos Titulares de Certificados emitidos pela AC INFOCOMEX, recomenda-se o uso de mecanismos que garantam a segurança computacional, tais como:

a) Senha de bios ativada;

b) Controle de acesso lógico ao sistema operacional;

c) Existência de uso de senhas fortes;

d) Diretivas de senha e de bloqueio de contas;

e) Antivírus, *antitrojan* e *antispyware* instalados, atualizados e habilitados;

f) Firewall pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;

g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix* etc); e

h) Proteção de tela acionada no máximo após cinco minutos de inatividade e exigindo senha do usuário para desbloqueio.

### 6.5.2 Classificação da segurança computacional

Não se aplica.

## 6.6. Controles Técnicos do Ciclo de Vida

A AC não exige um software específico para utilização dos certificados emitidos segundo esta PC.

### 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

Todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

## 6.7. Controles de Segurança de Rede

Os mesmos controles admitidos no item 6.7 da DPC.

## 6.8. Carimbo do Tempo

Não se aplica.

# 7. PERFIS DE CERTIFICADO, LCR E OCSP

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

## 7.1. Perfil do Certificado

Todos os certificados emitidos pela AC estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

### 7.1.1. Número de versão

Todos os certificados emitidos pela AC implementa 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. A ICP-Brasil define como obrigatórias as seguintes extensões:

| *Campo* | *Criticalidade* | *Valor* | *Presença* |
|---|---|---|---|
| ***Authority Key Identifier*** | ***Não crítica*** | Hash 160 bits SHA-1 da chave pública da AC que emite o certificado | Obrigatória |
| ***Subject KeyIdentifier*** | ***Não crítica*** | Hash 160 bits SHA-1 da chavepública da AC titular do certificado | Obrigatória |
| ***Key Usage*** | ***Crítica*** | *digitalSignature* | Obrigatória |
| | | *keyEncipherment* | Permitido |

| | | | |
|---|---|---|---|
| | | *nonRepudiation* | Permitido |
| ***Certificate Policies*** | ***Crítica*** | *PolicyIdentifier* OID *2.16.76.1.2.201.27* | Obrigatória |
| | | *Policyqualifiers* OID 1.3.6.1.5.5.7.2.1 | |
| | | *CPSurl:* http://repositorio.serpro.gov.br/docs/dpcacinfocomex.pdf | |
| ***Subject Alternative Name*** | ***Não crítica*** | OID = 2.16.76.1.3.3 e conteúdo =nas 14 (quatorze) posições o número do Cadastro Nacionalde Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado | Obrigatória * |
| ***Basic Constraints*** | ***Crítica*** | cA = False | Obrigatória |
| ***Extended Key Usage*** | ***Não crítica*** | *Client authentication OID* = 1.3.6.1.5.5.7.3.2 | Obrigatória |
| | | *E-mail protection OID = 1.3.6.1.5.5.7.3.4* | Permitido |
| ***CRL Distribution Points*** | ***Não crítica*** | *DistributionPointName* http://repositorio.serpro.gov.br/lcr/acinfocomexv2.crl http://certificados2.serpro.gov.br/lcr/acinfocomexv2.crl | Obrigatória |
| ***Authority Information Access*** | ***Não crítica*** | *id-ad-caIssuer* http://repositorio.serpro.gov.br/cadeias/accinfocomex.p7b | Obrigatória |

(*) A obrigatoriedade com restrição implica recomendação de manutenção desse otherName de forma provisória ,até 31/12/2028, com propósito de possibilitar que todas a aplicações possam ser ajustadas para obtenção dessa informação pelo atributo serialNumber(OID =2.5.4.5) do campo DN do titular após 31/12/2028,fica opcional o uso desse otherName. Outros otherNames podem ser utilizados, conforme defi nido ADE-ICP-04.01.

**Legenda: O = Obrigatório, P = Permitido e N = Não permitido**

7.1.2.2. Os campos otherName devem estar de acordo com as seguintes especificações:

a) o conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

b) quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CNO ou CAEPF não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF;

d) quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;

e) todas as informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) as 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita;

g) apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

h) não se aplica.

7.1.2.4. Os outros campos que compõem a extensão "Subject Alternative Name" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.5. Todas as informações utilizadas para preenchimento dos campos do certificado devem ser verificadas.

### 7.1.3. Identificadores de algoritmo

Os algoritmos criptográficos utilizados para assinatura dos certificados pela AC são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1]. Os certificados emitidos pela AC INFOCOMEX são assinados com o uso do algoritmo criptográfico SHA-256 com função de *hash* (**OID = 1.2.840.113549.1.1.11**).

### 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:

Para os certificados de selo eletrônico do tipo SE-S, será adotado o seguinte DN:

C = BR

O = ICP-Brasil

CN =<Razão Social>:CNPJserialNumber =<número CNPJ>

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

### 7.1.5. Restrições de nome

7.1.5.1. Neste item estão descritas as restrições aplicáveis para os nomes dos titulares dos certificados.

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

a) não são utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, são 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 **2.16.76.1.2.201.27** foi atribuído a esta Política de Certificado. Todo certificado emitido segundo esta PC contém, na extensão "*Certificate Policies*", o OID correspondente.

### 7.1.7. Uso da extensão "*Policy Constraints*"

Não se aplica.

### 7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC, o campo *policyQualifiers* da extensão "*Certificate Policies*" contém o endereço da página *web* com a DPC da AC. a saber:

| |
|---|
| http://repositorio.serpro.gov.br/docs/dpcacinfocomex.pdf |

### 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 de versão

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

### 7.2.2. Extensões de LCR e de suas entradas

7.2.2.1. A AC adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) *"**Authority Key Identifier"**,* **não crítica:** contém o *hash* SHA-1 da chave pública da AC; e

b) ***"CRL Number"*, não crítica**: contém número sequencial para cada LCR emitida.

7.2.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

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

b) ***"CRL Number"*, não crítica**: contém um número sequencial para cada LCR emitida.

### 7.3. Perfil de OCSP

Não se aplica.

#### 7.3.1. Número(s) de versão

Não se aplica.

#### 7.3.2. Extensões de OCSP

Não se aplica.

## 8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes na DPC da AC.

### 8.1. Frequência e circunstâncias das avaliações

### 8.2. Identificação/Qualificação do avaliador

### 8.3. Relação do avaliador com a entidade avaliada

### 8.4. Tópicos cobertos pela avaliação

### 8.5. Ações tomadas como resultado de uma deficiência

### 8.6. Comunicação dos resultados

## 9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens seguintes são referidos os itens correspondentes na DPC da AC.

### 9.1. Tarifas

#### 9.1.1. Tarifas de emissão e renovação de certificados

#### 9.1.2. Tarifas de acesso ao certificado

#### 9.1.3. Tarifas de revogação ou de acesso à informação de status

#### 9.1.4. Tarifas para outros serviços

**9.1.5. Política de reembolso**

**9.2. Responsabilidade Financeira**

**9.2.1. Cobertura do seguro**

**9.2.2. Outros ativos**

**9.2.3. Cobertura de seguros ou garantia para entidades finais**

**9.3. Confidencialidade da informação do negócio**

**9.3.1. Escopo de informações confidenciais**

**9.3.2. Informações fora do escopo de informações confidenciais**

**9.3.3. Responsabilidade em proteger a informação confidencial**

**9.4. Privacidade da informação pessoal**

**9.4.1. Plano de privacidade**

**9.4.2. Tratamento de informação como privadas**

**9.4.3. Informações não consideradas privadas**

**9.4.4. Responsabilidade para proteger a informação privadas**

**9.4.5. Aviso e consentimento para usar informações privadas**

**9.4.6. Divulgação em processo judicial ou administrativo**

**9.4.7. Outras circunstâncias de divulgação de informação**

**9.5. Direitos de Propriedade Intelectual**

**9.6. Declarações e Garantias**

**9.6.1. Declarações e Garantias da AC**

**9.6.2. Declarações e Garantias da AR**

**9.6.3. Declarações e garantias do titular**

**9.6.4. Declarações e garantias das terceiras partes**

**9.6.5. Representações e garantias de outros participantes**

**9.7. Isenção de garantias**

**9.8. Limitações de responsabilidades**

### 9.9. Indenizações

### 9.10. Prazo e Rescisão

### 9.10.1. Prazo

### 9.10.2. Término

### 9.10.3. Efeito da rescisão e sobrevivência

### 9.11. Avisos individuais e comunicações com os participantes

### 9.12. Alterações

### 9.12.1. Procedimento para emendas

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

### 9.12.2. Mecanismo de notificação e períodos

Mudança nesta PC será publicado no site da AC.

### 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 e AR e outras entidades citadas.

Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

### 9.16.2. Cessão

### 9.16.3. Independência de disposições

### 9.16.4. Execução (honorários dos advogados e renúncia de direitos)

### 9.17. Outras provisões

Esta PC foi submetida à aprovação, durante o processo de credenciamento da AC INFOCOMEX, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARACREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desseprocesso, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC.

# 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 |
|---|---|---|
| **[2]** | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL | **DOC-ICP-03** |
| **[3]** | 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 publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

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

# 11. REFERÊNCIAS BIBLIOGRÁFICAS

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

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

- 08/09/2026