# DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

# DA

# AUTORIDADE CERTIFICADORA DE DEFESA

## Assinatura Geral e
## Proteção de E-mail (S/MIME)

(DPC da AC DEFESA)

**Versão 3.1 de Maio de 2023**

**Infraestrutura de Chaves Públicas Brasileira**
**ICP - Brasil**

# Sumário

# CONTROLE DE ALTERAÇÕES

| Versão | Data | Motivo | Descrição da Alteração |
|---|---|---|---|
| **1.0** | 24/04/2017 | Versão Inicial | Versão inicial, de acordo com o DOC-ICP-05 versão 4.1. |
| **1.1** | 15/09/2017 | Atualização | Atualizado de acordo com o DOC-ICP-05 versão 4.2. |
| **2.0** | 31/10/2019 | Atualização | Atualizado de acordo com o DOC-ICP-05 versão 5.2. |
| **3.0** | 20/12/2022 | Atualização | Atualizado de acordo com o DOC-ICP-05 versão 6.3 |
| **3.1** | 12/06/2023 | Atualização | Atualizado pela AC DEFESA. Alteração/inclusão de endereços de publicação do repositório da AC Defesa e de suas LCR, de acordo com o DOC-ICP-05 versão 6.3 |

# 1 INTRODUÇÃO

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

## 1.1 Visão Geral

**1.1.1** Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e procedimentos a serem obrigatoriamente observados pela Autoridade Certificadora de Defesa (AC DEFESA), AC de primeiro nível integrante ICP-Brasil, na execução dos seus serviços de certificação digital.

**1.1.2** Esta DPC adota a estrutura recomendada pelo DOC-ICP-05 - Requisitos mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.

**1.1.3** A AC DEFESA não emite certificados SSL ou certificados CS.

**1.1.4** A estrutura desta DPC está baseada na RFC 3647.

**1.1.5** A AC DEFESA é responsável por manter as informações da DPC atualizadas, conforme registrado no Controle de Alterações.

## 1.2 Nome do documento e identificação

**1.2.1** Esta Declaração de Práticas de Certificação da Autoridade Certificadora de Defesa - DPC da AC DEFESA possui o Identificador de Objeto (OID) 2.16.76.1.1.92, atribuído pela ICP-Brasil.

**1.2.2** A AC DEFESA emite única e exclusivamente certificados para usuários finais, tendo como propósito de uso de chaves criptográficas a assinatura de documento e proteção de e-mail (S/MIME).

## 1.3 Participantes da ICP-Brasil

### 1.3.1 Autoridades Certificadoras

Esta DPC refere-se unicamente à AC DEFESA, integrante da ICP-Brasil .

### 1.3.2 Autoridades de Registro

**1.3.2.1** O endereço da página web (URL) da AC DEFESA é *https://www.acdefesa.mil.br*, onde estão publicados os dados a seguir, referentes às Autoridades de Registro (ARs) utilizadas pela AC DEFESA para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

a) relação de todas as Autoridades de Registro (AR) credenciadas; e

b) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

### 1.3.3 Titulares do certificado

Os titulares dos certificados emitidos podem ser pessoas físicas ou jurídicas, que atendam aos requisitos desta DPC e das Políticas de Certificado aplicáveis, devidamente autorizadas pela AR responsável a receber um certificado digital emitido pela AC DEFESA, para sua própria utilização ou para utilização em equipamentos e 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 Outros participantes

**1.3.5.1** A AC DEFESA publica em sua página web, *https://www.acdefesa.mil.br*, o Prestador de Serviços Biométricos - PSBios a ela vinculado.

## 1.4 Usabilidade do certificado

### 1.4.1 Uso apropriado do certificado

A AC DEFESA implementa as seguintes Políticas de Certificados, que definem como os certificados emitidos deverão ser utilizados. Nas PCs estão relacionadas as aplicações para as quais são adequados os certificados emitidos:

- Política de Certificado da AC DEFESA do Tipo A1 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A1, OID 2.16.76.1.2.1.78;
- Política de Certificado da AC DEFESA do Tipo A3 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A3, OID 2.16.76.1.2.3.75;
- Política de Certificado da AC DEFESA do Tipo A4 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A4, OID 2.16.76.1.2.4.44;
- Política de Certificado da AC DEFESA do Tipo S1 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica , PC AC DEFESA S1, OID 2.16.76.1.2.101.17;

- Política de Certificado da AC DEFESA do Tipo S3 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA S3, OID 2.16.76.1.2.103.15;
- Política de Certificado da AC DEFESA do Tipo S4 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA S4, OID 2.16.76.1.2.104.12.

### 1.4.2 Uso proibitivo do certificado

É vedada qualquer utilização do certificado que não esteja especificada na Política de Certificado da AC DEFESA associada ao certificado em questão.

## 1.5 Política de Administração

Neste item listar-se-á endereço e outras informações da AC DEFESA, responsável por esta DPC.

### 1.5.1 Organização administrativa do documento

Autoridade Certificadora de Defesa (AC DEFESA).

### 1.5.2 Contatos

**Nome:** Marcos Elias dos Prazeres Caetano
**Endereço:** Centro Integrado de Telemática do Exército - CITEx, Av. Duque de Caxias, s/n, Setor Militar Urbano, CEP 70630-100 - Brasília-DF
**Telefone:** (61) 2035-1076
**Página web:** https://www.acdefesa.mil.br
**E-mail:** contato@acdefesa.mil.br

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

**Nome:** André Luiz Cibin Ribeiro
**Telefone:** (61) 2035-1070
**E-mail:** andre@acdefesa.mil.br

### 1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI, de acordo com os procedimentos de aprovação estabelecidos a critério do Comitê Gestor da ICP-Brasil.

## 1.6 Definições e Acrônimos

| SIGLA | DESCRIÇÃO |
|---|---|
| AC | Autoridade Certificadora |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| ACP | Autoridade Certificadora Principal |
| ACR | Autoridade Certificadora Reserva |
| AR | Autoridades de Registro |
| CEI | Cadastro Específico do INSS |
| CF-e | Cupom Fiscal Eletrônico |
| CG | Comitê Gestor |
| CMM-SEI | Capability Maturity Model do Software Engineering Institute |
| CMVP | Cryptographic Module Validation Program |
| CN | Common Name |
| CNE | Carteira Nacional de Estrangeiro |
| CNPJ | Cadastro Nacional de Pessoas Jurídicas |
| COBIT | Control Objectives for Information and related Technology |
| COSO | Comitee of Sponsoring Organizations |
| CPF | Cadastro de Pessoas Físicas |
| CS | Code Signing |
| DMZ | Zona Desmilitarizada |
| DN | Distinguished Name |
| DPC | Declaração de Práticas de Certificação |
| EV | Extended Validation (WebTrust for Certification Authorities) |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IDS | Sistemas de Detecção de Intrusão |
| IEC | International Electrotechnical Commission |
| IETF PKIX | Internet Engineering Task Force - Public-Key Infrastructured (X.509) |
| ISO | International Organization for Standardization |
| ITSEC | European Information Technology Security Evaluation Criteria |
| ITU | International Telecommunications Union |
| LCR | Lista de Certificados Revogados |
| NBR | Norma Brasileira |
| NIS | Número de Identificação Social |
| NIST | National Institute of Standards and Technology |
| OCSP | On-line Certificate Status Protocol |

| SIGLA | DESCRIÇÃO |
|---|---|
| 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 |
| PIN | Personal Identification Number |
| PRD | Plano de Recuperação de Desastres |
| PRTI | Plano de Resposta e Tratamento de Incidentes |
| PIS | Programa de Integração Social |
| POP | Proof of Possession |
| PSBio | Prestador de Serviço Biométrico |
| PSC | Prestador de Serviço de Confiança |
| PSS | Prestadores de Serviço de Suporte |
| PUK | PIN Unbloking Key |
| RFC | Request for Comments |
| RG | Registro Geral |
| SAT | Sistema Autenticador e Transmissor |
| SGC | Sistema de Gerenciamento de Certificado |
| SNMP | Simple Network Management Protocol |
| SSL | Secure Socket Layer |
| TCSEC | Trusted System Evaluation Criteria |
| TSDM | Trusted Software Development Methodology |
| UF | Unidade da Federação |
| URL | Uniform Resource Location |

# 2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

## 2.1 Repositórios

**2.1.1** O repositório da AC DEFESA atende as seguintes obrigações:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC DEFESA e sua Lista de Certificados Revogados (LCR);

b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e

c) implementar os recursos necessários para a segurança dos dados nele armazenados.

**2.1.2** Requisitos aplicáveis aos repositórios utilizados pela AC DEFESA:

a) A AC DEFESA mantém seus repositórios disponíveis nos seguintes locais e endereços:
- *http://repositorio.acdefesa.mil.br* - AC Principal e AC Reserva;
- *http://repositorio-acp.acdefesa.mil.br* - AC Principal e AC Reserva;
- *http://repositorio-acr.acdefesa.mil.br* - AC Principal e AC Reserva;
- *https://repositorio-acp.acdefesa.mil.br* - AC Principal e AC Reserva; e
- *https://repositorio-acr.acdefesa.mil.br* - AC Principal e AC Reserva.

b) A disponibilidade da página e repositórios é de no mínimo 99,5% do mês;

c) Protocolos de acesso - HTTP e HTTPS; e

d) Obedece aos requisitos de segurança definidos no item 5 CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES.

**2.1.3** O repositório da AC DEFESA está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

**2.1.4** A AC DEFESA disponibiliza 02 (dois) repositórios para distribuição de LCR, em infraestruturas de rede segregadas, localizadas na AC Principal (Brasilia-DF) e AC Reserva (Rio de Janeiro-RJ), acessíveis nos seguintes endereços:

- *http://repositorio.acdefesa.mil.br/lcr*;
- *http://repositorio-acp.acdefesa.mil.br/lcr*;
- *http://repositorio-acr.acdefesa.mil.br/lcr*;
- *https://repositorio-acp.acdefesa.mil.br/lcr*; e
- *https://repositorio-acr.acdefesa.mil.br/lcr*

## 2.2 Publicação de informações dos certificados

**2.2.1** A AC DEFESA publica e mantém disponível em sua página *web* as informações descritas no item 2.2.2 no endereço (*https://www.acdefesa.mil.br*). A disponibilidade da página é de, no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

**2.2.2** As informações publicadas nas páginas da AC DEFESA são:

a) seu próprio certificado;

b) suas LCRs;

c) sua DPC;

d) as PCs que implementa;

e) relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços; e

f) relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

## 2.3 Tempo ou Frequência de publicação

**2.3.1** De modo a assegurar a disponibilização sempre atualizada de seus conteúdos, a AC DEFESA adota os seguintes prazos/frequência:

a) Os certificados e a LCR são publicados imediatamente após sua emissão;

b) As versões ou alterações desta DPC e das PCs são atualizadas no site da AC Defesa após aprovação da AC Raiz da ICP-Brasil;

c) A lista das AR vinculadas e seus endereços são publicadas sempre que sofrerem alterações.

## 2.4 Controle de acesso aos repositórios

**2.4.1** Não há qualquer restrição ao acesso *web* para consulta a esta DPC, a sua PC, aos certificados emitidos e à LCR da AC DEFESA. Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

# 3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC DEFESA verifica a autenticidade da identidade e/ou atributos de pessoas físicas e jurídicas da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As pessoas físicas e jurídicas estão proibidas de usar nomes em seus certificados que violem

os diretos de propriedade intelectual de terceiros. A AC DEFESA reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

## 3.1 Atribuição de Nomes

### 3.1.1 Tipos de nomes

**3.1.1.1** Os tipos de nomes admitidos para os titulares de certificados emitidos pela AC DEFESA são:

a) certificados de pessoa física, o campo *Common Name* (CN) é preenchido com o nome completo do Titular do Certificado, acrescido do caracter : e, em seguida, seu respectivo CPF;

b) certificados de pessoa jurídica, o campo *Common Name* (CN) é preenchido com o nome completo do órgão responsável pelo certificado, acrescido do caracter : e, em seguida, seu respectivo CNPJ.

**3.1.1.2** A AC DEFESA não emite certificado para ACs subsequentes.

### 3.1.2 Necessidade dos nomes serem significativos

Para identificação dos titulares dos certificados emitidos, a AC DEFESA faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem.

### 3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

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

**3.1.4.1** No âmbito da AC DEFESA, identificadores do tipo *Distinguished Name* (DN) devem ser únicos para cada titular de certificado. A AR pode propor e aprovar nomes distintos para candidatos de certificado.

**3.1.4.2** É vedado o uso de nomes nos certificados que violem os direitos de propriedade intelectual de terceiros.

### 3.1.5 Unicidade de nomes

Identificadores do tipo *Distinguished Name* (DN) devem ser únicos para cada titular de certificado e não ambíguos. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

### 3.1.6 Procedimento para resolver disputa de nomes

É reservado a AC DEFESA o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

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

Os processos de tratamento, reconhecimento e confirmação da autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

## 3.2 Validação inicial de identidade

Neste item e nos seguintes são descritos os requisitos e os procedimentos gerais utilizados pela AR, vinculada à AC DEFESA, responsável para a realização dos seguintes processos:

a) Identificação e cadastro inicial do titular do certificado - identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2 e 3.2.3, observado o quanto segue:

   i) para certificados de pessoa física: comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim.

   ii) para certificados de pessoa jurídica: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado, e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.

b) Emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

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

O Sistema de Gerenciamento de Certificados (SGC) implementado e utilizado pela AC DEFESA no gerenciamento do ciclo de vida de seus certificados, controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado.

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

Ao recebê-la, o SGC verifica automaticamente a assinatura digital com uso da chave pública incluída nessa solicitação. Esse teste confirma a posse da chave privada pelo requisitante. A solicitação, com seu número de identificação, é então armazenada no banco de dados do SGC.

Este número é impresso no Termo de Responsabilidade juntamente com os dados da entidade solicitante. Os dados são autenticados pela AR por meio da verificação das informações com base em originais de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

A AC DEFESA segue o padrão RFC 4210, relativo a POP (*Proof of Possession*).

### 3.2.2 Autenticação da Identificação da organização

#### 3.2.2.1 Disposições Gerais

**3.2.2.1.1** Os procedimentos empregados pela AR vinculada à AC DEFESA para a confirmação da identidade de uma pessoa jurídica são realizados mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

**3.2.2.1.2** Sendo titular do certificado uma pessoa jurídica, será designada pessoa física responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou o procurador constituído na forma do item 3.2, alínea 'a', inciso (ii) acima.

**3.2.2.1.3** Será feita a confirmação da identidade da organização e da pessoa física, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.2.2.2;

b) apresentação do rol de documentos elencados no item 3.2.3.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

c) coleta e verificação biométrica da pessoa física responsável pelo certificado, conforme regulamentos expedidos, por meio de instruções normativas, pela AC Raiz, que definam os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil, bem como os procedimentos para identificação biométrica na ICP-Brasil; e

d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo responsável pelo certificado.

**Nota 1:** A AR poderá solicitar uma assinatura manuscrita ao requerente ou responsável pelo uso do certificado em termo específico para a comparação com o documento de identidade ou contrato social. Nesse caso, o termo manuscrito digitalizado e assinado digitalmente pelo AGR será apensado ao dossiê eletrônico do certificado, podendo o original em papel ser descartado.

**3.2.2.1.4** Fica dispensado o disposto no item 3.2.2.1.3, alíneas 'b' e 'c', caso o responsável pelo certificado possua certificado digital de pessoa física ICP-Brasil válido, do tipo A3 ou superior, com os dados biométricos devidamente coletados, e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

**3.2.2.1.5** O disposto no item 3.2.2.1.3 deverá ser realizado mediante comparecimento presencial do representante legal.

### 3.2.2.2 Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) Relativos à sua habilitação jurídica:

   i) se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;

   ii) se entidade privada, não se aplica. A AC DEFESA não emite certificados para entidades privadas.

b) relativos à sua habilitação fiscal:

   i) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ; ou

   ii) prova de inscrição no Cadastro Específico do INSS - CEI.

**Nota 1:** As confirmações que tratam o item 3.2.2.2 poderão ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais de órgão competente. É obrigatório essas validações constarem no dossiê eletrônico do titular do certificado.

### 3.2.2.3 Informações contidas no certificado emitido para uma organização

**3.2.2.3.1** É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;;[1]

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[2]

c) Nome completo do responsável pelo certificado, sem abreviações;[3]

d) Data de nascimento do responsável pelo certificado;[4];

e) Cadastro de Pessoa Física (CPF) do responsável pelo certificado; e

f) E-mail do responsável pelo certificado.

[1]No campo Subject, como parte do Common Name, que compõe o Distinguished Name
[2]No campo Subject Alternative Name, OID 2.16.76.1.3.3
[3]No campo Subject Alternative Name, OID 2.16.76.1.3.2
[4]No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.4

**3.2.2.3.2** Cada PC pode definir como obrigatório o preenchimento de outros campos, ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.2.3.2.

#### 3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização

Os atos praticados com o certificado digital de titularidade de uma organização estão sujeitos ao regime de responsabilidade definido em lei quanto aos poderes de representação conferidos ao responsável de uso indicado no certificado.

### 3.2.3 Autenticação da identidade de um indivíduo

A confirmação deverá ser realizada mediante a presença física do interessado ou por meio de módulo eletrônico da AR, o qual deverá assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

#### 3.2.3.1 Procedimento para identificação de um indivíduo

A identificação da pessoa física requerente do certificado emitido pela AC Defesa deverá ser realizada como segue:

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital:

   i) Cédula de identidade militar, se militar;

   ii) Registro de identidade, se brasileiro; ou

   iii) Título de Eleitor, com foto; ou

   iv) Carteira nacional de estrangeiro - CNE, se estrangeiro domiciliado no Brasil; ou

   v) Passaporte, se estrangeiro não domiciliado no Brasil.

b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil.

**Nota 1:** Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, conforme admitido pela legislação específica, emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, incluindo carteiras de identidades emitidas por órgãos de identificação das Forças Armadas, desde que contenham fotografia.

**3.2.3.1.1** Na hipótese de identificação positiva por meio do processo biométrico da ICP-Brasil fica dispensada a apresentação de qualquer dos documentos elencados no item 3.2.3.1 e a etapa de verificação. As evidências desse processo farão parte do dossiê eletrônico do requerente.

**3.2.3.1.2** Os documentos digitais serão verificados por meio de barramentos ou aplicações oficiais dos entes federativos. Tal verificação fará parte do dossiê eletrônico do titular do certificado. Na hipótese da identificação positiva, fica dispensada a etapa de verificação conforme o item 3.2.3.1.3.

**3.2.3.1.3** Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, serão verificados:

a) por agente de registro distinto do que realizou a etapa de identificação;

b) pela AR DEFESA; e

c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

**3.2.3.1.4** A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente, e as normas editadas pelo Comitê Gestor da ICP-Brasil.

**3.2.3.1.5** Para a identificação de indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto no item 3.2.9.3.

**3.2.3.1.6** Não se aplica

**3.2.3.1.7** Não se aplica.

**3.2.3.1.8** A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade.

**3.2.3.1.8.1** Não se aplica.

### 3.2.3.2 Informações contidas no certificado emitido para um indivíduo.

**3.2.3.2.1** É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

a) nome completo sem abreviações[1];

[1]No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*

b) data de nascimento[2];e

c) Cadastro de Pessoa Física (CPF)[3].

**3.2.3.2.1.1** Não se aplica.

**3.2.3.2.2** A AC DEFESA define como obrigatório o preenchimento do campo E-mail do usuário na emissão dos certificados.

**Nota**: Os campos abaixo são opcionais e serão preenchidos mediante solicitação do titular do certificado e declaração expressa no termo de titularidade:

a) número do Registro Geral - RG do titular e órgão expedidor;

b) número de Identificação Social - NIS (PIS, PASEP ou CI);

c) número do Cadastro Específico do INSS (CEI) ou CAEPF; e

d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor.

e) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

**3.2.3.2.3** O titular deve apresentar a documentação respectiva, caso a caso, em sua versão original. A AC DEFESA manterá arquivo com as cópias de todos os documentos utilizados.

**Nota 1:** É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

**Nota 2:** O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

**3.2.3.2.3.1** Não se aplica.

### 3.2.4 Informações não verificadas do titular do certificado

Não se aplica.

### 3.2.5 Validação das autoridades

Não se aplica.

[2]No campo *Subject Alternative Name*, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.1

[3]No campo *Subject Alternative Name*, nas 11(onze) posições subsequentes às 8 (oito) posições reservadas à data de nascimento, o Cadastro Pessoa Física (CPF) - OID 2.16.76.1.3.1

### 3.2.6 Critérios para interoperação

Não se aplica.

### 3.2.7 Autenticação da identidade de equipamento ou aplicação

#### 3.2.7.1 Disposições gerais

A AC DEFESA não emite certificados para equipamentos ou aplicações.

#### 3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

Não se aplica.

#### 3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação

Não se aplica.

#### 3.2.7.4 Autenticação de identificação de equipamento para certificado CF-e-SAT

Não se aplica.

#### 3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT

Não se aplica.

#### 3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT

Não se aplica.

#### 3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR

Não se aplica.

#### 3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico

Não se aplica.

#### 3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico

Não se aplica.

### 3.2.8 Procedimentos complementares

**3.2.8.1** A AC DEFESA mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC DEFESA é membro, bem como os Requisitos de Linha de Base.

**3.2.8.2** Todo o processo de identificação do titular do certificado será registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC DEFESA, com a utilização de certificado digital ICP-Brasil do tipo A3. O sistema biométrico da ICP-BRASIL solicitará aleatoriamente qual dedo o AGR deverá apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGR no cadastro do sistema biométrico. Tais registros serão feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

**3.2.8.2.1** Não se aplica.

**3.2.8.3** Será mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias serão mantidas em papel ou em forma digitalizada, tendo sido observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

**3.2.8.3.1** Não se aplica.

**3.2.8.3.2** Não se aplica.

**3.2.8.3.3** Não se aplica.

**3.2.8.4** As AC DEFESA disponibilizará, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03[6] e DOC-ICP-05.02 [10].

**3.2.8.4.1** Na hipótese de identificação positiva no processo biométrico da ICP-Brasil, ficará dispensada a apresentação de qualquer documentação de identidade do requerente ou da etapa de verificação conforme item 3.2.3.1.

**3.2.8.4.2** Não se aplica.

### 3.2.9 Procedimentos específicos

**3.2.9.1** Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no item 3.2, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

**3.2.9.2** Disposições para a Validação de Solicitação de Certificados do Tipo A CF-e-SAT:

Não se aplica.

**3.2.9.3** A solicitação de certificado para servidores públicos federais da ativa e militares da União seguirá o abaixo descrito:

a) realizar a validação do registro por meio de processo de individualização inequívoca e eletrônica do servidor público federal da ativa e militar da União por meio de seus respectivos sistemas eletrônicos de gestão de pessoas, feita na presença de servidor ou militar autorizador, a ser definido pelos órgãos competentes, que formalmente será cadastrado no sistema da AC autorizada, e, assim, ser o responsável a confirmar a emissão de certificados dessa natureza;

b) os servidores públicos federais da ativa e militares da União deverão ter sido biometricamente identificados e individualizados pela base biométrica oficial do TSE ou pelos PSBios credenciados da ICP-Brasil ou base oficial equivalente, com comprovação auditável do cadastro desses requerentes por parte da AC DEFESA. Essa comprovação poderá ser pelo CPF ou outro indexador viável entre os sistemas;

c) obter os dados do servidor público federal da ativa e militar da União por via de seus respectivos sistemas eletrônicos de gestão de pessoas, sem que haja qualquer possibilidade de alteração desses, para que sejam enviados para a AC DEFESA emitir o certificado digital; e

d) ser assinada por autoridade designada pelos respectivos órgãos gestores de pessoas, sendo a AC DEFESA responsável por manter cadastro atualizado das autoridades competentes e respectivas autorizações e/ou requisições para fins de auditoria e fiscalização.

**3.2.9.3.1** Módulo Eletrônico da AR dos Órgãos Gestores de Pessoas
A AR vinculada à AC DEFESA, representada pelo módulo eletrônico da AR dos órgãos gestores de pessoas, deve:

a) ser um sistema vinculado à AC DEFESA, AC credenciada pela ICP-Brasil, de acordo com esta Instrução Normativa;

b) possuir, de forma segura, registros de trilhas de auditoria;

c) comunicar diretamente utilizando protocolos de comunicação seguro com os sistemas determinados formalmente pelos órgãos gestores de pessoas, pelo Tribunal Superior Eleitoral ou pelo Prestador de Serviço Biométrico ou pelo custodiante de outra base biométrica oficial;

d) ter sido auditada pelo ITI em procedimento pré-operacional;

e) possuir as listas atualizadas com os nomes e CPF ou outro indexador dos servidores públicos, dos militares e dos autorizadores, com a comprovação auditável da resposta do sistema biométrico do Tribunal Superior Eleitoral ou prestadores de serviço biométrico ou pelo custodiante de outra base biométrica oficial. Os autorizadores são formalmente designados pelos órgãos competentes, por instrumento normativo.

**Nota:** Ficam excepcionalizados para as AR descritas no item 3.2.9.3.1 os requisitos dispostos no DOC-ICP-03.01[1].

**3.2.9.3.2** Aplica-se o disposto no item 3.2.9.3 aos servidores públicos estaduais e do Distrito Federal, da ativa, desde que as Unidades da Federação as quais estejam vinculados:

a) possuam Sistema de Gestão de Pessoal capaz de realizar a validação do registro por meio de processo de individualização inequívoca e eletrônica do servidor público da ativa;

b) identifiquem biometricamente os servidores públicos pela base biométrica oficial do TSE, pelos PSBios credenciados da ICP-Brasil ou base oficial equivalente, com comprovação auditável desses cadastros; e

c) possuam uma AR credenciada junto a ICP-Brasil e que disponibilize um módulo de AR que atenda aos requisitos previstos no item 3.2.9.3.1.

**3.2.9.3.3** Não se aplica

**3.2.9.3.4** Apenas as Autoridades Certificadoras autorizadas a emitirem certificados para servidores públicos da ativa e militares da União estão obrigadas a alterar suas DPCs e PCs, submetendo-as à aprovação do ITI.

**3.2.9.4** Não se aplica.

**3.2.9.5** Não se aplica.

**3.2.9.6** Não se aplica.

**3.2.9.7** Não se aplica.

**3.2.9.8** Não se aplica.

## 3.3 Identificação e autenticação para pedidos de novas chaves

**3.3.1** Neste item são estabelecidos os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC DEFESA para a geração de novo par de chaves e de seu novo certificado.

**3.3.2** Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3;

b) solicitação por meio eletrônico, na página da AC DEFESA, opção "Gerenciamento de Certificado", assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) não se aplica;

d) não se aplica;

e) não se aplica; e

f) não se aplica.

**3.3.2.1** A AC DEFESA não emite certificado para equipamento ou aplicação.

**3.3.3** Caso sejam requeridos procedimentos específicos para as PC implementadas, os mesmos devem ser descritos nessas PC, no item correspondente.

**3.3.4** A AC DEFESA não possui AC de nível subsequente.

## 3.4 Identificação e Autenticação para solicitação de revogação

O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.9.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Raiz.
A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR DEFESA.

As solicitações podem ser feitas por escrito, em formulário específico ou por meio eletrônico, na página da AC DEFESA, opção "Gerenciamento de Certificado".

O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.9.3. Solicitações de revogação de certificados devem ser registradas.

As razões para revogação do certificado sempre serão registradas e informadas para o seu titular.

# 4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

## 4.1 Solicitação do certificado

Os requisitos e procedimentos mínimos necessários, estabelecidos pela AC DEFESA e pelas ARs a ela vinculadas, para as solicitações de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.2;

b) o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes ao de um certificado de tipo A3, a autenticação biométrica do agente de registro responsável pelas solicitações de emissão e de revogação de certificados; ou quando da emissão para servidores públicos da ativa e militares da União, Estados e Distrito Federal, por servidor público e militar autorizado pelos sistemas de gestão de pessoal dos órgãos competentes; e

c) um termo de titularidade assinado digitalmente pelo titular do certificado ou pelo responsável pelo uso do certificado, no caso de certificado de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico, e, ainda, quando emissão para servidor público da ativa e militar da União, Estados e Distrito Federal pela autoridade designada formalmente pelos órgãos competentes; e

d) não se aplica.

**Nota 1:** A AC DEFESA não emite certificados de usuários finais com propósito de uso EV SSL ou EV CS.
**Nota 2:** A AC DEFESA não emite certificados SSL, de equipamento, aplicação,*codesign* e carimbo de tempo.

### 4.1.1 Quem pode submeter uma solicitação de certificado

A submissão da solicitação deve ser sempre por intermédio da AR.

#### 4.1.1.1 Não se aplica.

#### 4.1.1.2 Não se aplica.

#### 4.1.1.3 Não se aplica.

#### 4.1.1.4 Não se aplica.

### 4.1.2 Processo de registro e responsabilidades

Descrever-se-á nos itens a seguir as obrigações gerais das entidades envolvidas, explicitando, se houver, as obrigações específicas para as PCs implementadas nos itens correspondentes.

#### 4.1.2.1 Responsabilidades da AC DEFESA

**4.1.2.1.1** A AC DEFESA responde pelos danos a que der causa.

**4.1.2.1.2** A AC DEFESA responde solidariamente pelos atos das entidades de sua cadeia de certificação: ARs e PSS.

**4.1.2.1.3** Quando da emissão de certificado digital para servidores públicos da ativa e militares da União, Estados e Distrito Federal autorizados pelos responsáveis dos respectivos órgãos competentes, a responsabilidade por qualquer irregularidade na identificação do requerente do certificado incidirá sobre o órgão responsável pela identificação.

#### 4.1.2.2 Obrigações da AC DEFESA

Descrever-se-á nos itens a seguir as obrigações da AC DEFESA, AC responsável por esta DPC:

a) operar de acordo com esta DPC e com as PC que implementa;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de AR a ela vinculada e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCR;

k) publicar em página *web* a DPC e as PC aprovadas que implementa;

l) publicar em página *web* as informações definidas no item 2.2.2 deste documento;

m) publicar em página *web* as informações sobre o descredenciamento de AR;

n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

t) à AC DEFESA, por ser órgão da Administração Direta da União, não cabe a contratação de seguro de responsabilidade civil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas condicionantes e limitações determinadas pela legislação vigente;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;

w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;

x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada à AC DEFESA; e

y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados ou por módulo eletrônico da AR.

#### 4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

#### 4.1.2.4 Obrigações das ARs

As obrigações da AR vinculada à AC DEFESA são as abaixo relacionadas:

a) operar de acordo com esta DPC e com as PC que implementa;

b) receber solicitações de emissão ou de revogação de certificados;

c) confirmar a identidade do solicitante e a validade da solicitação;

d) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC DEFESA utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];

e) informar aos respectivos titulares a emissão ou a revogação de seus certificados;

f) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC DEFESA e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1], bem como Princípios e Critérios *WebTrust* para AR [5];

g) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;

h) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2 e 3.2.3; e

i) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios *WebTrust* para AR [5].

## 4.2 Processamento de Solicitação de Certificado

### 4.2.1 Execução das funções de identificação e autenticação

A AC DEFESA e a AR à ela vinculada executam as funções de identificação e autenticação conforme o item 3 desta DPC.

### 4.2.2 Aprovação ou rejeição de pedidos de certificado

**4.2.2.1** Não se aplica.

**4.2.2.2** A AC e AR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes, de acordo com os procedimentos descritos nesta DPC.

### 4.2.3 Tempo para processar a solicitação de certificado

A AC DEFESA cumprirá os procedimentos determinados na ICP-Brasil. Não haverá tempo máximo para processar as solicitações na ICP-Brasil.

## 4.3 Emissão de Certificado

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

**4.3.1.1** Os certificados são emitidos pela AC DEFESA de acordo com os seguintes passos:

a) o responsável pela AR verifica o completo e correto preenchimento da solicitação do certificado e a apresentação da documentação do solicitante;

b) o responsável pela AR aprova a solicitação, o sistema da AC DEFESA emite e disponibiliza o certificado para instalação para o solicitante e o titular é notificado por e-mail.

**4.3.1.2** O certificado é considerado válido a partir do momento de sua emissão.

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

O titular do certificado será notificado por e-mail após o processo de emissão do certificado, conforme item 4.3.1.1.

## 4.4 Aceitação de Certificado

### 4.4.1 Conduta sobre a aceitação do certificado

**4.4.1.1** O titular do certificado ou pessoa física responsável, verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. No caso de não aceitar o certificado o titular não poderá utiliza-lo e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado ou pessoa física responsável pelo certificado de pessoas jurídicas:

a) concorda com as responsabilidades, obrigações e deveres impostas no Termo de Responsabilidade, nesta DPC e na PC correspondente;

b) declara que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

c) afirma que todas as informações fornecidas durante o processo de solicitação são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

**4.4.1.2** A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, na assinatura do Termo de Titularidade pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

**4.4.1.3** Não se aplica.

### 4.4.2 Publicação do certificado pela AC

O certificado da AC DEFESA é publicado de acordo com o item 2.2 desta DPC.

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

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

## 4.5 Usabilidade do par de chaves e do certificado

O titular do certificado para usuário final emitido pela AC DEFESA deve operar de acordo com esta Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) da AC DEFESA, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

**4.5.1.1** A AC DEFESA utilizará sua chave privada e garantirá a proteção dessa chave conforme o previsto nesta DPC.

**4.5.1.2** Obrigações do titular do certificado.

As obrigações do titular de certificado emitido pela AC DEFESA, de acordo com esta DPC, constantes dos termos de titularidade de que trata o item 4.1, são as abaixo relacionados:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (*PIN*) e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

d) conhecer os seus direitos e obrigações, contemplados pela DPC da AC DEFESA e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e

e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

f) garantir a proteção do *PUK*, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

**Nota:** Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado.

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

Em acordo com o item 9.6.4 desta DPC.

## 4.6 Renovação de Certificados

Em acordo com o item 3.3 desta DPC.

### 4.6.1 Circunstâncias para renovação de certificados

Em acordo com o item 3.3 desta DPC.

### 4.6.2 Quem pode solicitar a renovação

Em acordo com o item 3.3 desta DPC.

### 4.6.3 Processamento de requisição para renovação de certificados

Em acordo com o item 3.3 desta DPC.

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

Em acordo com o item 3.3 desta DPC.

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

Em acordo com o item 3.3 desta DPC.

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

Não se aplica.

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

Em acordo com o item 4.3 desta DPC.

## 4.7 Nova chave de certificado (Re-key)

### 4.7.1 Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

## 4.8 Modificação de certificado

Não se aplica.

### 4.8.1 Circunstâncias para modificação de certificado

Não se aplica.

### 4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica.

### 4.8.3 Processamento de requisição de modificação de certificado

Não se aplica.

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

Não se aplica.

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

Não se aplica.

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

Não se aplica.

#### 4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

Não se aplica.

## 4.9 Suspensão e Revogação de Certificado

### 4.9.1 Circunstâncias para revogação

**4.9.1.1** A AC DEFESA pode revogar um certificado por ela emitido pelos seguintes motivos:

a) exoneração ou suspensão do titular, no caso de certificado de pessoa jurídica;

b) mudança de cargo, função ou permissões do titular, no caso de certificado de pessoa jurídica;

c) falha do titular no cumprimento de suas obrigações ou qualquer compromisso, regulamento ou lei em vigor;

d) solicitação de um dos responsáveis descritos no item 4.9.2;

e) devolução da mídia armazenadora do certificado.

**4.9.1.2** Um certificado é revogado obrigatoriamente pelos seguintes motivos:

a) quando constatada emissão imprópria ou defeituosa do mesmo;

b) quando for necessária a alteração de qualquer informação nele contida;

c) no caso de dissolução de AC;

d) no caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

**4.9.1.3** Em relação à revogação, esta DPC também observa que:

a) a AC DEFESA revogará, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil; e

b) o CG da ICP-Brasil ou a AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

**4.9.1.4** Todo certificado terá sua validade verificada, na respectiva LCR, antes de ser utilizado.

**4.9.1.4.1** Não se aplica.

**4.9.1.4.2** Não se aplica.

**4.9.1.5** A autenticidade da LCR será confirmada por meio das verificações de assinatura da AC DEFESA, emitente, e do período de validade da LCR.

### 4.9.2 Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente poderá ser feita:

a) pelo titular do certificado;

b) pelo responsável do certificado, no caso de certificado de pessoas jurídicas;

c) pelo órgão, quando o titular do certificado for seu empregado, funcionário ou servidor, no caso de certificado de pessoas jurídicas;

d) pela AC DEFESA;

e) por uma AR vinculada à AC DEFESA;

f) por determinação do CG da ICP-Brasil ou da AC Raiz;

g) não se aplica;

h) por servidores públicos da ativa e militares da União, Estados e Distrito Federal autorizados pelos respectivos órgãos competentes pela identificação dos mesmos;

i) não se aplica;

j) não se aplica.

### 4.9.3 Procedimento para solicitação de revogação

**4.9.3.1** Todos agentes habilitados, conforme o item 4.9.2, podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados. O procedimento para a solicitação de uma revogação varia dependendo de quem a origina, e pode ser realizada de duas formas:

a) por intermédio da página *web* da AC DEFESA na opção “Gerenciamento de Certificado”, autenticando-se com o próprio certificado digital, se dentro da validade ou informando o ”identificador”do certificado e a ”frase senha”; ou

b) envio do formulário específico existente no endereço que foi utilizado para solicitação. O formulário deverá ser encaminhado devidamente preenchido.

**4.9.3.2** Como diretrizes gerais, esta DPC estabelece que:

a) o solicitante da revogação de um certificado deve ser identificado;

b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;

c) as justificativas para a revogação de um certificado são documentadas;

d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o número de série do certificado revogado.

**4.9.3.3** O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

**4.9.3.4** Não se aplica.

**4.9.3.5** A AC DEFESA responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

**4.9.3.6** Caso sejam requeridos procedimentos de revogação específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

### 4.9.4 Prazo para solicitação de revogação

**4.9.4.1** A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.1.

**4.9.4.2** Não se aplica.

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

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC DEFESA processará a revogação imediatamente após a análise do pedido.

### 4.9.6 Requisitos de verificação de revogação para as partes confiáveis

Antes de confiar em um certificado, a parte confiável deve confirmar a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs ou respostas OCSP identificados em cada certificado na cadeia de certificação.

### 4.9.7 Frequência de emissão de LCR

**4.9.7.1** As LCR referentes aos certificados emitidos pela AC DEFESA são geradas a cada 1 (uma) hora.

**4.9.7.2** A frequência máxima admitida para a emissão de LCR para os certificados de usuário finais é de 6 (seis) horas.

**4.9.7.3** Não se aplica.

**4.9.7.4** Não se aplica.

**4.9.7.5** Não se aplica.

### 4.9.8 Latência máxima para a LCR

A LCR é divulgada no repositório em no máximo 4 (quatro) horas após sua geração.

### 4.9.9 Disponibilidade para revogação/verificação de status on-line

A AC DEFESA não suporta o processo de verificação da situação de estado de certificados de forma online (OCSP). O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 3.4.

### 4.9.10 Requisitos para verificação de revogação on-line

Não se aplica

### 4.9.11 Outras formas disponíveis para divulgação de revogação

**4.9.11.1** A AC não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

**4.9.11.2** Não se aplica.

### 4.9.12 Requisitos especiais para o caso de comprometimento de chave

**4.9.12.1** Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a AC DEFESA e solicitar a revogação de seu certificado conforme descrito no item 4.9.3.

**4.9.12.2** A comunicação com a AC DEFESA poderá ser efetuada por telefone, e-mail ou presencial junto à AR vinculada à AC DEFESA.

### 4.9.13 Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de usuários finais.

### 4.9.14 Quem pode solicitar suspensão

Não se aplica.

#### 4.9.15 Procedimento para solicitação de suspensão

Não se aplica.

#### 4.9.16 Limites no período de suspensão

Não se aplica.

### 4.10 Serviços de status de certificado

#### 4.10.1 Características operacionais

A AC DEFESA adota como ponto de distribuição da LCR os endereços definidos no tópico 2.1.2. Conforme especificado no item 4.9.9, a AC DEFESA não suporta o processo de verificação da situação de estado de certificados de forma online (OCSP).

#### 4.10.2 Disponibilidade dos serviços

Ver item 4.9

#### 4.10.3 Funcionalidades operacionais

Ver item 4.9

### 4.11 Encerramento de atividades

**4.11.1** Caso seja necessária a extinção dos serviços de AC ou AR, a AC DEFESA efetuará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-Brasil [6].

**4.11.2** Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos, incluem:

a) Notificação para o e-mail do titular do certificado;

b) Transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;

c) Preservação de quaisquer registros não transferidos a um sucessor;

d) As chaves públicas dos certificados emitidos pela AC DEFESA serão armazenadas por outra AC após aprovação da AC Raiz;

e) Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC DEFESA;

f) A AC DEFESA, caso encerre suas atividades, transferirá a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e

g) Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

## 4.12 Custódia e recuperação de chave

### 4.12.1 Política e práticas de custódia e recuperação de chave

Não é permitido a recuperação de chaves privadas de sigilo da AC DEFESA.

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

Não se aplica.

# 5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes descrever-se-ão os controles de segurança implementados pela AC DEFESA e pela AR a ela vinculada para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

## 5.1 Controles Físicos

Nos itens a seguir são descritos os controles físicos referentes às instalações que abrigam os sistemas da AC DEFESA e instalações da AR vinculada.

### 5.1.1 Construção e localização das instalações de AC

**5.1.1.1** A localização e o sistema de certificação utilizado para a operação da AC DEFESA não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

**5.1.1.2** Todos os aspectos de construção das instalações da AC DEFESA, relevantes para os controles de segurança física, foram executadas por técnicos especializados, passam por manutenção periódica, especialmente os itens descritos abaixo:

a) instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia,

subestações, retificadores e estabilizadores e similares;

b) instalações para sistemas de telecomunicações;

c) sistema de aterramento e de proteção contra descargas atmosféricas; e

d) iluminação de emergência.

O ambiente principal de produção é situado em sala-cofre construída de acordo com os requisitos e normas da ABNT. Possui, assim, todos os dispositivos exigidos na norma.

### 5.1.2 Acesso físico

O acesso físico às dependências da AC DEFESA é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

#### 5.1.2.1 Níveis de Acesso

**5.1.2.1.1** São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC DEFESA, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

**5.1.2.1.2 O primeiro nível - ou nível 1** - situa-se após a primeira barreira de acesso às instalações da AC DEFESA. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC DEFESA deverão transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC DEFESA é executado nesse nível.

**5.1.2.1.3** Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC DEFESA, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e só poderão ser utilizados mediante autorização formal e supervisão.

**5.1.2.1.4 O segundo nível - ou nível 2** - é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC DEFESA. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

**5.1.2.1.5 O terceiro nível - ou nível 3** - é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC DEFESA. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer

nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

**5.1.2.1.6** No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, com o cartão eletrônico, e a identificação biométrica.

**5.1.2.1.7** Telefones celulares, bem como quaisquer outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC DEFESA, não são admitidos a partir do nível 3.

**5.1.2.1.8 O quarto nível - ou nível 4** - é interno ao terceiro nível. É onde ocorrem as atividades especialmente sensíveis de operação da AC DEFESA, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

**5.1.2.1.9** No quarto nível, as paredes, piso e o teto são inteiriços e revestidos de aço e concreto, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 - que constituem a chamada sala-cofre - possuem proteção contra interferência eletromagnética externa.

**5.1.2.1.10** A sala-cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

**5.1.2.1.11** São dois os ambientes de quarto nível localizados na sala cofre, abrigando os seguintes itens:

a) sala de equipamentos de suporte (ar-condicionado e quadros de distribuição);

b) sala de equipamentos de produção *on-line*, equipamentos de rede e infraestrutura (*firewall, switches,* roteadores e servidores) e cofre de armazenamento.

**5.1.2.1.12 O quinto nível - ou nível 5** - é interno aos ambientes de nível 4, e é compreendido por cofre. Materiais criptográficos, tais como, chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

**5.1.2.1.13** Para garantir a segurança do material armazenado, o cofre obedece às seguintes especificações mínimas:

a) é feito em aço ou material de resistência equivalente;

b) possui tranca com chave.

**5.1.2.1.14** **O sexto nível - ou nível 6** - consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da chave privada da AC DEFESA estão armazenados em um desses depósitos.

### 5.1.2.2 Sistema físico de detecção

**5.1.2.2.1** Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

**5.1.2.2.2** Os vídeos resultantes da gravação 24x7 são armazenadas por, no mínimo, 7 (sete) anos. Eles são testados (verificação de trechos aleatórios no início, meio e final dos vídeos) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um lote de arquivos de vídeo referente a cada semana. Esses vídeos são armazenadas em ambiente de terceiro nível.

**5.1.2.2.3** Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

**5.1.2.2.4** Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

**5.1.2.2.5** O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

**5.1.2.2.6** O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações.

### 5.1.2.3 Sistema de Controle de Acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

#### 5.1.2.4 Mecanismos de emergência

**5.1.2.4.1** Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC DEFESA em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

**5.1.2.4.2** Todos os procedimentos referentes aos mecanismos de emergência estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

### 5.1.3 Energia e ar-condicionado

**5.1.3.1** A infraestrutura do ambiente de certificação da AC DEFESA é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC DEFESA e seus respectivos serviços. Um sistema de aterramento está implantado.

**5.1.3.2** Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados.

**5.1.3.3** São utilizadas tubulações, dutos, calhas, quadros e caixas - de passagem, de distribuição e de terminação - projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

**5.1.3.4** Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 (seis) meses, na busca de evidências de violação ou de outras anormalidades.

**5.1.3.5** São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Qualquer modificação nessa rede é previamente documentada.

**5.1.3.6** Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

**5.1.3.7** O sistema de climatização atende aos requisitos de temperatura e umidade exigida pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante a falhas.

**5.1.3.8** A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

**5.1.3.9** O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

**5.1.3.10** A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC é garantida por meio de:

a) geradores de porte compatível;

b) geradores de reserva;

c) sistemas de *no-breaks* redundantes; e

d) sistemas redundantes de ar-condicionado.

### 5.1.4 Exposição à água

A estrutura inteiriça do ambiente de nível 4, construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

### 5.1.5 Prevenção e proteção contra incêndio

**5.1.5.1** Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

**5.1.5.2** Nas instalações da AC DEFESA não é permitido fumar ou portar objetos que produzam fogo ou faísca.

**5.1.5.3** A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre são eclusas, onde uma porta só se abre quando a anterior está fechada.

**5.1.5.4** Em caso de incêndio nas instalações da AC DEFESA, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

### 5.1.6 Armazenamento de mídia

A AC DEFESA atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

### 5.1.7 Destruição de lixo

**5.1.7.1** Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

**5.1.7.2** Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

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

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em condições idênticas, no máximo, 48 (quarenta e oito) horas.

## 5.2 Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC DEFESA e nas ARs a ela vinculadas, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

### 5.2.1 Perfis qualificados

**5.2.1.1** A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um militar ou funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada funcionário estão limitadas de acordo com o seu perfil.

**5.2.1.2** A AC DEFESA estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

**5.2.1.3** Todos os operadores do sistema de certificação da AC DEFESA recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

**5.2.1.3.1** Não se aplica.

**5.2.1.4** Quando um empregado se desliga da AC, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação com todos os recursos inicialmente disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

### 5.2.2 Número de pessoas necessário por tarefa

**5.2.2.1** O Requisito de controle multiusuário é requerido para a geração e a utilização da chave privada da AC DEFESA, conforme o descrito em 6.2.2.

**5.2.2.2** Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC DEFESA necessitam da presença de, no mínimo 2 (dois) operadores (funcionários) com perfis qualificados. As demais tarefas da AC DEFESA podem ser executadas por um único operador.

### 5.2.3 Identificação e autenticação para cada perfil

**5.2.3.1** Pessoas que ocupam os perfis designados pela AC DEFESA passam por um processo rigoroso de seleção. Todo funcionário da AC DEFESA tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC DEFESA;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC DEFESA;

c) receber um certificado para executar suas atividades operacionais na AC DEFESA; e

d) receber uma conta no sistema de certificação da AC DEFESA.

**5.2.3.2** Os certificados, contas e senhas utilizadas para identificação e autenticação dos funcionários:

a) são diretamente atribuídos a um único operador (funcionário) da AC DEFESA devidamente qualificado;

b) não são compartilhados; e

c) são restritos às ações associadas ao perfil para o qual foram criados.

**5.2.3.3** A AC DEFESA implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

### 5.2.4 Funções que requerem separação de deveres

A AC DEFESA impõem a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

## 5.3 Controles de Pessoal

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC DEFESA, pelas AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os integrantes da AC DEFESA e das AR e PSS

vinculados, encarregados de tarefas operacionais, têm registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocupam;

b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

c) o compromisso de observar as normas, políticas e regras aplicáveis da AC DEFESA; e

d) o compromisso de não divulgar informações sigilosas a que tenham acesso.

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

Todo o pessoal da AC DEFESA e AR vinculadas envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e na Política de Segurança da AC DEFESA.

### 5.3.2 Procedimentos de verificação de antecedentes

**5.3.2.1** Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC DEFESA e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, são submetidos aos seguintes processos, antes do começo das atividades:

a) VERIFICAÇÃO de antecedentes criminais;

b) VERIFICAÇÃO de situação de crédito;

c) VERIFICAÇÃO de histórico de empregos anteriores; e

d) COMPROVAÇÃO de escolaridade e de residência.

**5.3.2.2** A AC DEFESA poderá definir requisitos adicionais para a verificação de antecedentes.

### 5.3.3 Requisitos de treinamento

Todo o pessoal da AC DEFESA e das AR vinculadas, envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC DEFESA e das AR vinculadas;

b) sistema de certificação em uso na AC DEFESA;

c) procedimentos de recuperação de desastres e de continuidade do negócio;

d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do itens 3.2.2 e 3.2.3; e

e) outros assuntos relativos a atividades sob sua responsabilidade.

### 5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC DEFESA e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC DEFESA ou das ARs. Treinamentos de reciclagem são realizados pela AC DEFESA sempre que necessário.

### 5.3.5 Frequência e sequência de rodízios de cargos

A AC DEFESA não implementa rodízio de cargos.

### 5.3.6 Sanções para ações não autorizadas

**5.3.6.1** Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC DEFESA ou de uma ARs vinculada, a AC DEFESA suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação e instaurará processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

**5.3.6.2** O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

a) relato da ocorrência com *"modus operandi"*;

b) identificação dos envolvidos;

c) eventuais prejuízos causados;

d) punições aplicadas, se for o caso; e

e) conclusões.

**5.3.6.3** Concluído o processo administrativo, a AC DEFESA encaminhará suas conclusões à AC Raiz.

**5.3.6.4** As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;

b) suspensão por prazo determinado; ou

c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

### 5.3.7 Requisitos para designação de pessoal

O pessoal da AC DEFESA e das ARs vinculadas envolvido no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é designado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC DEFESA pode definir requisitos adicionais para a designação.

### 5.3.8 Documentação fornecida ao pessoal

**5.3.8.1** A AC DEFESA disponibiliza para todo o seu pessoal e para o pessoal das ARs vinculadas, no mínimo:

a) esta DPC;

b) as PCs que implementa;

c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];

d) a Política de Segurança da AC DEFESA;

e) documentação operacional relativa a suas atividades;

f) contratos, normas e políticas relevantes para suas atividades.

**5.3.8.2** Toda a documentação fornecida ao pessoal é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC DEFESA.

## 5.4 Procedimentos de Log de Auditoria

Descrever-se-á no itens seguintes os aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC DEFESA com o objetivo de manter o ambiente seguro.

### 5.4.1 Tipos de Evento Registrados

**5.4.1.1** Todas as ações executadas pelo pessoal da AC DEFESA, no desempenho de suas atribuições, são registradas em arquivos de auditoria de modo que cada ação esteja associada à pessoa que a realizou. A AC DEFESA registra em arquivos para fins de auditoria os seguintes eventos relacionados à segurança do seu sistema de certificação:

a) iniciação e desligamento do sistema de certificação;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC DEFESA;

c) mudanças na configuração da AC DEFESA ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

e) tentativas de acesso (*login*) e de saída do sistema (*logoff*);

f) tentativas não autorizadas de acesso aos arquivos de sistema;

g) geração de chaves próprias da AC DEFESA ou de chaves de Titulares de Certificados;

h) emissão e revogação de certificados;

i) geração de LCR;

j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;

k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;

l) operações de escrita nesse repositório, quando aplicável.

**5.4.1.1.1** Não se aplica.

**5.4.1.2** A AC DEFESA registra, eletrônica ou manualmente, as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e de perfis qualificados;

d) relatórios de discrepância e comprometimento; e

e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

**5.4.1.3** Os registros de auditoria mínimos a serem mantidos pela AC DEFESA incluem, além dos acima:

a) registros de solicitação, inclusive registros relativos a solicitações rejeitadas;

b) pedidos de geração de certificado, mesmo que a geração não tenha êxito; e

c) registros de solicitação de emissão de LCR.

**5.4.1.4** Todo o registro de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

**5.4.1.5** Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC DEFESA é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

**5.4.1.6** As ARs vinculadas a AC DEFESA registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos, obrigatórios, estão incluídos em arquivos de auditoria:

a) os agentes de registro que realizam as operações;

b) data e hora das operações;

c) a associação entre os agentes que realizam a validação e aprovação e o certificado gerado; e

d) a assinatura digital do executante.

**5.4.1.6.1** Não se aplica.

**5.4.1.7** A AC Defesa armazena eletronicamente as cópia dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e cópia dos termos de titularidade, itens que compõem o dossiê dos titulares de certificados. O local de arquivamento está definido em documento que faz parte da lista de documentos disponibilizados para as auditorias de conformidade.

### 5.4.2 Frequência de auditoria de registros

A periodicidade de auditoria de registros não será superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC DEFESA. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros para verificar se não foram alterados. Em seguida, procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

### 5.4.3 Período de Retenção para registros de Auditoria

A AC DEFESA mantém localmente, em suas próprias instalações, os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, faz o armazenamento da maneira descrita no item 5.5.

### 5.4.4 Proteção de registros de Auditoria

**5.4.4.1** Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

**5.4.4.2** As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção.

Esses registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

**5.4.4.3** Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

### 5.4.5 Procedimentos para cópia de segurança (*backup*) de registro de auditoria

A AC DEFESA executa procedimentos de *backup*, de todo o sistema de certificação (Sistema Operacional, Sistema de Aplicação e Banco de Dados) de duas formas:

a) diariamente: cópia de segurança;

b) semanalmente: cópia armazenada para processos de auditoria.

### 5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

O sistema de coleta de dados de auditoria é interno à AC DEFESA e compreende a combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação da AC, pelo sistema de controle de acesso e pelo pessoal operacional da AC. A descrição dos itens estão listados na tabela abaixo:

| **Tipo de Evento** | **Sistema de coleta** | **Registrado Por** |
|---|---|---|
| Sucesso e fracasso de tentativas de mudanças nos parâmetros de segurança do sistema operacional | Automático | Sistema operacional |
| Início e parada de aplicação | Automático | Sistema operacional |
| Sucesso e fracasso de tentativas de log-in e log-out | Automático | Sistema operacional |
| Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema | Automático | Sistema operacional |
| Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados | Automático | Sistema operacional |
| Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados | Automático | *Software* de AC ou de AR |
| Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado | Automático | *Software* de AR |
| *Logs de Backup* e de restauração | Automático e manual | Sistema operacional/ pessoal de operações. |
| Mudanças de configuração de sistema | Manual | Pessoal de Operações |
| Atualizações de *software* e *hardware* | Manual | Pessoal de Operações |
| Manutenção de sistema | Manual | Pessoal de Operações |
| Mudanças de pessoal | Manual | Pessoal de Operações |
| Registros de acessos físicos | Automático e manual | *Software* de controle de acesso/pessoal de operações |

### 5.4.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC DEFESA não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

### 5.4.8 Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC DEFESA, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas pela AC DEFESA para fins de auditoria.

## 5.5 Arquivamento de registros

### 5.5.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC DEFESA:

a) solicitações de certificados;

b) solicitações de revogação de certificados;

c) notificações de comprometimento de chaves privadas;

d) emissões e revogações de certificados;

e) emissões de LCR;

f) trocas de chaves criptográficas da AC DEFESA;

g) informações de auditoria previstas no item 5.4.1.

### 5.5.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

a) as LCR e os certificados de assinatura digital são retidos permanentemente para fins de consulta histórica;

b) os dossiês dos titulares devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e

c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 7 (sete) anos.

### 5.5.3 Proteção de arquivo

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

### 5.5.4 Procedimentos de cópia de arquivo

**5.5.4.1** Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC DEFESA, e recebe o mesmo tipo de proteção utilizada no arquivo principal.

**5.5.4.2** As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

**5.5.4.3** É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

### 5.5.5 Requisitos para datação de registros

**5.5.5.1** Os servidores de dados utilizados pela AC DEFESA são sincronizados com a hora GMT fornecida pela Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário GMT, inclusive os certificados emitidos por esses equipamentos.

**5.5.5.2** No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

### 5.5.6 Sistema de coleta de dados de arquivo (interno e externo)

Todos os sistemas de coleta de dados de arquivos utilizados pela AC DEFESA são internos, sendo uma combinação de procedimentos operacionais automatizados e manuais, executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional, conforme a seguir:

| Tipo de Evento | Sistema de coleta | Registrado Por |
|---|---|---|
| Solicitações de certificados | Automático e Manual | *Software* de AC e de AR / pessoal de operações |
| Solicitações de revogação de certificados | Automático e Manual | *Software* de AC e de AR / pessoal de operações |
| Emissões e revogações de certificados | Automático | *Software* de AC e de AR |
| Emissões de LCR | Automático | *Software* de AC |
| Notificações de comprometimento de chaves privadas | Manual | Pessoal de operações |

### 5.5.7 Procedimentos para obter e verificar informação de arquivo

As informações de arquivos da AC DEFESA e ARs vinculadas podem ser acessadas da seguinte forma:

a) por pessoas autorizadas e corretamente identificadas, mediante apresentação de um instrumento devidamente constituído;

b) por titulares de certificados ou seus representantes legais, mediante solicitação formal;

c) a própria AC por meio de seus funcionários ou os Agentes de Registros das ARs vinculadas.

## 5.6 Troca de chave

**5.6.1** A AC DEFESA comunica ao Titular de Certificado, por *e-mail*, a necessidade de renovação do certificado, com antecedência de 45 dias da expiração do certificado válido, com instruções para a renovação do certificado. A solicitação de renovação deverá ser feita pelo próprio Titular do Certificado quando do recebimento dessa notificação, por meio eletrônico, assinado digitalmente com o uso do certificado vigente a ser renovado.

**5.6.2** No caso de procedimentos ou prazos específicos para as PCs implementadas, os mesmos são descritos nessas PCs, no item correspondente.

## 5.7 Comprometimento e Recuperação de Desastre

Nos itens a seguir estão relacionados procedimentos de notificação e de recuperação de desastres previstos no Plano de Continuidade de Negócio (PCN) da AC DEFESA, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

### 5.7.1 Procedimentos de gerenciamento de incidente e comprometimento

**5.7.1.1** A AC DEFESA possui um Plano de Continuidade do Negócio - PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos, conforme explicitado no tópico 4.1.2.2. A AC DEFESA possui ainda um Plano de Resposta a Incidentes (PRI) e um Plano de Recuperação de Desastres (PRD).

**5.7.1.2** No PCN das ARs vinculadas à AC DEFESA são previstos os seguintes procedimentos para recuperação total ou parcial das atividades das ARs:

a) identificação dos eventos que causaram interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;

b) identificação e concordância de todas as responsabilidades e procedimentos de emergência;

c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;

d) documentação dos processos e procedimentos acordados;

e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e

f) teste e atualização dos planos.

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

No PCN da AC DEFESA é previsto as ações e procedimentos de recuperação utilizados quando recursos computacionais, *software* ou dados são corrompidos ou quando houver suspeita de corrupção, resumidos em:

a) identificação de todos os elementos corrompidos;

b) determinação do instante do comprometimento, fator crítico para invalidar as transações executadas após aquele instante;

c) análise do nível do comprometimento para a determinação das ações a serem executadas. As ações podem variar de uma simples restauração de um *backup* de segurança, passando por acionamento da contingência da AC DEFESA até a revogação do certificado da AC DEFESA.

### 5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

#### 5.7.3.1 Certificado de entidade é revogado

A AC DEFESA possui um PCN que especifica as ações a serem tomadas no caso em que seu certificado tenha que ser revogado. Tais procedimentos podem ser resumidos em:

a) a AC DEFESA revoga todos os certificados por ela emitidos e emite uma nova LCR;

b) a AC Raiz é informada por meio de comunicação segura e é solicitado a revogação do certificado da AC DEFESA e a emissão de um novo certificado;

c) os titulares de certificados emitidos pela AC DEFESA são notificados sobre a revogação dos certificados;

d) é acionada a contingência e restabelecido os serviços de AC; e

e) iniciam-se os procedimentos para emissão dos novos certificados de usuários.

**Nota:** Os titulares de certificados são instruídos a solicitar um novo certificado que será validado e aprovado de acordo com esta DPC.

#### 5.7.3.2 Chave de entidade é comprometida

No PCN da AC DEFESA está especificado que, em caso de comprometimento da chave da AC DEFESA, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas para ativar a contingência da AC.

### 5.7.4 Capacidade de continuidade de negócio após desastre

A AC DEFESA possui um Plano de Recuperação de Desastres (PRD) que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro. O propósito deste plano é restabelecer as principais operações da AC DEFESA quando a operação de sistemas é significativamente e adversamente abalada por fogo, inundação, greves, etc.

## 5.8 Extinção da AC DEFESA

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

# 6 CONTROLES TÉCNICOS DE SEGURANÇA

Descrever-se-á neste tópico as medidas de segurança implantadas pela AC DEFESA para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados, além de outros controles técnicos de segurança utilizados pela AC DEFESA e suas ARs vinculadas na execução de suas funções operacionais.

## 6.1 Geração e Instalação do Par de Chaves

### 6.1.1 Geração do Par de Chaves

**6.1.1.1** O par de chaves criptográficas da AC DEFESA é gerado por ela própria, em módulo criptográfico de *hardware* com padrão de segurança conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

**6.1.1.2** Somente os titulares dos certificados emitidos pela AC DEFESA geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC DEFESA.

**6.1.1.3** Cada PC implementada pela AC DEFESA define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

**6.1.1.4** O processo de geração do par de chaves da AC DEFESA é feito por *hardware*.

**6.1.1.5** Cada PC implementada pela AC DEFESA caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

**6.1.1.6** Esta DPC descreve os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC DEFESA. Os padrões de referência são os definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 6.1.2 Entrega da chave privada à entidade

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 emissor de certificado

**6.1.3.1** A AC DEFESA entregará à AC RAIZ cópia de sua chave pública, em formato PKCS#10. Essa entrega será feita por representante legal da AC DEFESA, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz.

**6.1.3.2** Chaves públicas são entregues ao emissor de certificado por intermédio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC DEFESA.

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

As formas para a disponibilização do certificado da AC DEFESA, e de todos os certificados da cadeia de certificação, para os usuários da AC DEFESA, compreendem:

a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];

b) página *web* da AC DEFESA *(https://www.acdefesa.mil.br)*;

c) outros meios seguros aprovados pelo CG da ICP-Brasil.

### 6.1.5 Tamanhos de chave

**6.1.5.1** As PC implementadas pela AC DEFESA definirão os tamanhos das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

**6.1.5.2** Não se aplica.

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

**6.1.6.1** Os parâmetros de geração de chaves assimétricas da AC DEFESA seguem o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

**6.1.6.2** A verificação dos parâmetros de geração de chave é feita de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

**6.1.7.1** Os certificados de assinatura emitidos pela AC DEFESA têm ativados os bits *digitalSignature, nonRepudiation e keyEncipherment* enquanto que os certificados de sigilo têm ativados apenas os bits *dataEncipherment e keyEncipherment*. Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC DEFESA, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

**6.1.7.2** A chave privada da AC DEFESA é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

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

Nos itens seguintes são definidos os requisitos para a proteção das chaves privadas da AC DEFESA. A chave privada da AC DEFESA é gerada, armazenada e utilizada apenas em *hardware* criptográfico específico, que atende o padrão "Homologação da ICP-Brasil NSH-3", não havendo tráfego em nenhum momento.

### 6.2.1 Padrões para módulo criptográfico

**6.2.1.1** O módulo criptográfico de geração de chaves assimétricas da AC DEFESA adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]. O módulo criptográfico segue o padrão "Homologação da ICP-Brasil NSH-3". Novos módulos devem ser homologados pelo INMETRO conforme estabelecido pela ICP-Brasil.

**6.2.1.2** Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] - Cada PC implementada especifica os requisitos adicionais aplicáveis.

### 6.2.2 Controle "*n* de *m*" para chave privada

**6.2.2.1** A AC DEFESA implementa o controle múltiplo, do tipo (n) pessoas de um grupo de (m), para a ativação e a desativação da sua chave privada por intermédio de controles de acesso físico e do *software* de certificação.

**6.2.2.2** É exigida a presença, no mínimo, de 2 (dois) detentores da chave de ativação (n) de um grupo de 11 (onze) (m) para a ativação da chave da AC DEFESA.

### 6.2.3 Custódia *(escrow)* de chave privada

Não existe, no contexto da AC DEFESA, a recuperação *(escrow)* de chaves privadas, isto é, não se permite que terceiros obtenham uma chave privada sem o consentimento de seu titular. Assim sendo, não existe agente de recuperação.

### 6.2.4 Cópia de segurança de chave privada.

**6.2.4.1** Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

**6.2.4.2** A AC DEFESA mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave aprovado pelo CG da ICP-Brasil e mantida pelo prazo de validade do certificado correspondente.

**6.2.4.3** A AC DEFESA não mantém cópia de segurança das chaves privadas de titulares de certificados por ela emitidos.

**6.2.4.4** A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

### 6.2.5 Arquivamento de chave privada

**6.2.5.1** As chaves privadas dos titulares de certificados emitidos pela AC DEFESA não são arquivadas.

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

### 6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da AC DEFESA é inserida no módulo criptográfico de acordo com os procedimentos especificados pelo fornecedor do módulo, segundo o estabelecido na RFC 4210 e 6712.

### 6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

### 6.2.8 Método de ativação de chave privada

A ativação da chave privada da AC DEFESA é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "11" dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são militares integrantes das Forças Armadas indicados pela AC DEFESA para essa função. As senhas utilizadas obedecem à política de senhas estabelecida pela AC DEFESA.

### 6.2.9 Método de desativação de chave privada

A chave privada da AC DEFESA, armazenada em módulo criptográfico, é desativada quando não é mais necessária, através de mecanismo disponibilizado pelo *software* de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "11" dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são militares integrantes das Forças Armadas indicados pela AC DEFESA para essa função. As senhas utilizadas obedecem à política de senhas por ele estabelecida.

### 6.2.10 Método de destruição de chave privada

Quando a chave privada da AC DEFESA for desativada, em decorrência de expiração ou revogação, esta será eliminada da memória do módulo criptográfico. Qualquer espaço em memória, onde a chave estava armazenada, será sobrescrito. Todas as cópias de segurança da chave privada da AC DEFESA e os cartões criptográficos dos detentores serão destruídos. Os agentes autorizados para realizar estas operações são os administradores de sistema e os detentores das chaves de ativação da AC DEFESA, que são identificados individualmente por meio de cartão *smartcard* contendo chaves criptografadas de acesso ao módulo criptográfico.

## 6.3 Outros Aspectos do Gerenciamento do Par de Chaves

### 6.3.1 Arquivamento de chave pública

A AC DEFESA armazena as chaves públicas da própria AC DEFESA e dos titulares de certificados de assinatura digital, bem como as LCR emitidas 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 DEFESA e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes . A chave pública da AC DEFESA pode ser 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** Os períodos de uso das chaves correspondentes aos certificados de sigilo emitidos pela AC DEFESA são definidos nas respectivas PCs.

**6.3.2.3** As PCs implementadas pela AC DEFESA definem o período máximo de validade de seus certificados com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

**6.3.2.4** O período máximo de validade admitido para o certificado da AC DEFESA é de 10 (dez) anos.

## 6.4 Dados de Ativação

Nos itens seguintes, são 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. Os requisitos específicos, quando existirem, serão descritos nas PCs correspondentes.

### 6.4.1 Geração e instalação dos dados de ativação

**6.4.1.1** A AC DEFESA garante que os dados de ativação da sua chave privada são únicos e aleatórios.

**6.4.1.2** Todas as PCs implementadas garantem que os dados de ativação da chave privada do titular do certificado, se utilizados, são únicos e aleatórios.

### 6.4.2 Proteção dos dados de ativação.

**6.4.2.1** Os dados de ativação da chave privada da AC DEFESA são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

**6.4.2.2** Todas as PCs implementadas garantem que 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

Item não aplicável.

## 6.5 Controles de Segurança Computacional

### 6.5.1 Requisitos técnicos específicos de segurança computacional

**6.5.1.1** A AC DEFESA garante que a geração de seu par de chaves é realizada em ambiente *off-line*, para impedir o acesso remoto não autorizado.

**6.5.1.2** Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficos dos titulares de certificados emitidos pela AC DEFESA estão descritos no item 6.5.1 das PC implementadas.

**6.5.1.3** Os computadores servidores, utilizados pela AC DEFESA, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis da AC DEFESA;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC DEFESA;

c) acesso restrito aos bancos de dados da AC DEFESA;

d) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

e) geração e armazenamento de registros de auditoria da AC DEFESA;

f) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;

g) mecanismos para cópias de segurança *(backup).*

**6.5.1.4** Essas características são implementadas pelo sistema operacional ou por meio da combinação deste, com o sistema de certificação e com mecanismos de segurança física.

**6.5.1.5** Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem apagadas as informações sensíveis nele contidas é sera efetuado o controle de entrada e saída, com o registro do número de série e as datas de envio e de recebimento. Ao retornar às instalações onde reside é inspecionado. Todo equipamento que deixar de ser utilizado em caráter permanente terão suas informações sensíveis relativas à atividade da AC DEFESA destruídas de maneira definitiva. Todos esses eventos são registrados para fins de auditoria.

**6.5.1.6** Qualquer equipamento incorporado à AC DEFESA é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

### 6.5.2 Classificação da segurança computacional

Não se aplica.

### 6.5.3 Controle de segurança para as Autoridades de Registro

**6.5.3.1** Os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas ARs para os processos de validação e aprovação de certificados são os previstos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

**6.5.3.2** São incluídos, pelo menos, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

**6.5.3.3** Não se aplica.

## 6.6 Controles Técnicos do Ciclo de Vida

Nos itens seguintes são descritos, quando aplicáveis, os controles implementados pela AC DEFESA e pelas ARs a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

### 6.6.1 Controles de desenvolvimento de sistemas

**6.6.1.1** A AC DEFESA adota um Sistema de Certificação Digital baseado em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Após a finalização do processo de homologação das customizações é necessária a avaliação do Chefe da AC Principal, que decide quando será a implementação no ambiente de produção.

**6.6.1.2** Os processos de projeto e desenvolvimento conduzidos pela AC DEFESA proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DEFESA.

### 6.6.2 Controle de gerenciamento de segurança

**6.6.2.1** A AC DEFESA verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas por intermédio da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência são tomadas as medidas para recuperação da situação conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

**6.6.2.2** A AC DEFESA utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema, antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

a) Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;

b) Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e

c) Instalação de novos serviços na plataforma de processamento.

### 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 checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação ao número da LCR, data/hora de emissão e outras informações relevantes.

## 6.7 Controles de Segurança de Rede

### 6.7.1 Diretrizes Gerais

**6.7.1.1** Os controles implementados para garantir a confidencialidade, a integridade e a disponibilidade dos serviços da AC DEFESA em ambiente de rede são os seguintes:

a) os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs, switches, firewalls* e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores *web* do sistema de certificação da AC DEFESA estão localizados e operam em ambiente protegido por três perímetros de segurança: os dois primeiros controlados por vigilantes e o terceiro constituído por controle de acesso biométrico;

b) as versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções e atualizações, disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação;

c) o acesso lógico aos elementos de infraestrutura e proteção de rede é restrito por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo;

d) infraestrutura de conectividade, incluindo:

   1) alojamento seguro de equipamento de comunicação;

   2) *firewall* seguro e serviços de roteamento;

   3) serviço de LAN seguro;

   4) serviço *back office* seguro;

5) serviço de Internet seguro e redundante.

e) prevenção de incidentes e avaliação, incluindo:

1) descoberta de intrusão;

2) análise de vulnerabilidades;

3) configuração segura de servidor;

4) auditorias técnicas.

f) administração de infraestrutura, incluindo:

1) monitoramento de servidor;

2) monitoramento de rede;

3) monitoramento de URL;

4) relatórios de níveis de serviço.

**6.7.1.2** Nos servidores e elementos de infraestrutura e proteção de rede utilizada pela AC DEFESA, somente os serviços estritamente necessários são habilitados.

**6.7.1.3** Os servidores e elementos de infraestrutura e proteção de rede tais como roteadores, *hubs, switches, firewalls* e sistemas de detecção de intrusão (IDS) localizados no segmento de rede que hospeda o sistema de certificação da AC DEFESA, estão localizados e operam em ambiente de nível 4.

**6.7.1.4** As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções e atualizações, disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação.

**6.7.1.5** O acesso lógico aos elementos de infraestrutura e proteção de rede é restringido por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

### 6.7.2 *Firewall*

**6.7.2.1** Mecanismos de *firewall* estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O *firewall* promove o isolamento, por intermédio de zona desmilitarizada, em sub-redes específicas dos equipamentos servidores com acesso externo em relação aos equipamentos com acesso exclusivamente interno à AC DEFESA.

**6.7.2.2** O *software de firewall*, entre outras características, implementa registros de auditoria.

### 6.7.3 Sistema de detecção de intrusão (IDS)

**6.7.3.1** O IDS implementado na AC DEFESA tem capacidade de reconhecer ataques em tempo real e respondê-los automaticamente com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

**6.7.3.2** O IDS tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

**6.7.3.3** O IDS provê registros de eventos *(log)*, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

### 6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado em roteadores, *firewalls* ou IDS, são registradas em arquivos de *log* para análise. A frequência de exame dos arquivos de *log* é diária e todas as ações tomadas em decorrência desse exame são documentadas.

## 6.8 Carimbo de Tempo

Não se aplica.

# 7 PERFIS DE CERTIFICADO, LCR E OCSP

## 7.1 Perfil do Certificado

Todos os certificados emitidos pela AC DEFESA estão em conformidade com o formato definido pelo padrão ITU X. 509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280.

### 7.1.1 Número de versão

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

### 7.1.2 Extensões de certificados

Não se aplica. A AC DEFESA não emite certificados de AC.

### 7.1.3 Identificadores de algoritmos

Não se aplica. A AC DEFESA não emite certificados de AC.

#### 7.1.4 Formatos de nome

Não se aplica. A AC DEFESA não emite certificados de AC.

#### 7.1.5 Restrições de nome

Não se aplica. A AC DEFESA não emite certificados de AC.

#### 7.1.6 OID *(Object Identifier)* de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC DEFESA após conclusão do processo de seu credenciamento é **2.16.76.1.1.92**.

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

Não se aplica. A AC DEFESA não emite certificados de AC.

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

O campo *policyQualifiers* da extensão "*Certificate Policies*" contém o endereço *web* *http://repositorio.acdefesa.mil.br/docs/dpc-acdefesa.pdf* da DPC da AC DEFESA.

#### 7.1.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

### 7.2 Perfil de LCR

#### 7.2.1 Número(s) de versão

As LCR geradas pela AC DEFESA 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** AC DEFESA adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

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

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***, deve conter o hash SHA-1 da chave pública da AC que assina a LCR; e

b) ***CRL Number***, não crítica: deve conter um número sequencial para cada LCR emitida pela AC.

## 7.3 Perfil de OCSP

### 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

## 8.1 Frequência e circunstâncias das avaliações

A AC DEFESA, enquanto entidade integrante da ICP-Brasil, sofreu auditoria prévia, para fins de credenciamento, e sofre auditorias anuais, para fins de manutenção de credenciamento.

## 8.2 Identificação/Qualificação do avaliador

**8.2.1** As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

**8.2.2** Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

## 8.3 Relação do avaliador com a entidade avaliada

As auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

## 8.4 Tópicos cobertos pela avaliação

**8.4.1** As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust.*

**8.4.2** Para fins de credenciamento na ICP-Brasil, a AC DEFESA recebeu auditoria prévia da AC Raiz e tem como previsto ser auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

**8.4.3** A entidade da ICP-Brasil diretamente vinculada à AC DEFESA (AR DEFESA) também recebeu auditoria prévia, para fins de credenciamento, sendo a AC DEFESA responsável pela realização de auditorias anuais nessa entidade, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

## 8.5 Ações tomadas como resultado de uma deficiência

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

## 8.6 Comunicação dos resultados

Em acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

# 9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

## 9.1 Tarifas

### 9.1.1 Tarifas de emissão e renovação de certificados

A AC DEFESA não cobra tarifas para emissão e renovação de certificados por ela emitidos.

### 9.1.2 Tarifas de acesso ao certificado

Não há cobrança de tarifas sobre este serviço.

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

Não há tarifa de revogação ou de acesso à informação de status de certificado.

### 9.1.4 Tarifas para outros serviços

Não se aplica.

### 9.1.5 Política de reembolso

Não se aplica.

## 9.2 Responsabilidade Financeira

A responsabilidade da AC DEFESA será verificada conforme previsto na legislação brasileira.

### 9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

### 9.2.2 Outros ativos

Conforme regramento desta DPC.

### 9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

## 9.3 Confidencialidade da informação do negócio

### 9.3.1 Escopo de informações confidenciais

**9.3.1.1** Considerar-se-á como informação sigilosa pela AC DEFESA, responsável por esta DPC e pelas ARs a ela vinculadas, todas àquelas informações coletadas, geradas, transmitidas e mantidas pela AC DEFESA e ARs a ela vinculadas que não foram especificadas no tópico 9.3.2 desta DPC.

**9.3.1.2** O princípio geral, estabelecido por esta DPC, é o de que nenhum documento, informação ou registro fornecido à AC DEFESA ou às ARs a ela vinculadas deverá ser divulgado.

### 9.3.2 Informações fora do escopo de informações confidenciais

As informações e documentos considerados não sigilosos pela AC DEFESA, responsável por esta DPC, e pelas ARs a ela vinculadas, são os seguintes:

a) os certificados e as LCRs emitidos pela AC DEFESA;

b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;

c) as PCs implementadas pela AC DEFESA;

d) a DPC da AC DEFESA;

e) versões públicas de PS;

f) a conclusão dos relatórios de auditoria; e

g) todo o conteúdo de livre acesso disponibilizado na página *web* da AC DEFESA.

**9.3.2.1** Certificados, LCR e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não confidenciais.

**9.3.2.2** Os seguintes documentos da AC também são considerados documentos não confidenciais:

a) qualquer PC aplicável;

b) qualquer DPC;

c) versões públicas de Política de Segurança - PS; e

d) a conclusão dos relatórios de auditoria.

**9.3.2.3** A AC DEFESA se reserva o direito de divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados emitidos no âmbito da ICP-Brasil.

### 9.3.3 Responsabilidade em proteger a informação confidencial

**9.3.3.1** Os participantes que recebem ou tem acesso a informações confidenciais possuem mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

**9.3.3.2** A chave privada de assinatura digital da AC DEFESA, AC credenciada responsável pela DPC, foi gerada pela própria AC DEFESA, sendo também por ela mantida, sendo responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC DEFESA é sua inteira responsabilidade.

**9.3.3.3** A AC DEFESA informa, através desta DPC, que os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. A AC DEFESA informa ainda que esses se responsabilizam pela divulgação ou utilização indevidas dessas mesmas chaves.

**9.3.3.3.1** No intuito de preservar o sigilo da sua chave privada, o titular pelo certificado deve tomar todas as medidas para a proteção da mesma. O sigilo da chave privada do certificado é garantido através de senha de acesso à chave privada. Esta senha será definida pelo usuário no momento da instalação do certificado. A criação e utilização dessa senha para acesso à aplicação são de responsabilidade do usuário. O titular do certificado deve observar procedimentos básicos de segurança, tais como:

a) nunca fornecer a senha a terceiros;

b) utilizar senha de, no mínimo, 8 caracteres;

c) não utilizar senha fraca ou óbvia, conforme definido na Política de Segurança da AC DEFESA, item 5;

d) montar senha com caractere numéricos e alfanuméricos;

e) memorizar a senha e não escrevê-la;

f) guardar a mídia principal e cópia de segurança em lugar seguro.

**9.3.3.4** A AC DEFESA informa, através desta DPC, que os titulares de certificados de sigilo emitidos para pessoas físicas ou os responsáveis pelo uso de certificados de sigilo emitidos para pessoas jurídicas, são responsáveis pela manutenção e pela garantia do sigilo das respectivas chaves privadas desses certificados, conforme especificado no item correspondente das PCs implementadas.

## 9.4 Privacidade da informação pessoal

### 9.4.1 Plano de privacidade

A AC DEFESA assegura a proteção de dados pessoais, conforme sua Política de Privacidade.

### 9.4.2 Tratamento de informação como privadas

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

### 9.4.3 Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR da AC DEFESA.

### 9.4.4 Responsabilidade para proteger a informação privadas

A AC DEFESA e as ARs a ela vinculadas são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

### 9.4.5 Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC DEFESA poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou

b) por meio de pedido escrito com firma reconhecida.

### 9.4.6 Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC DEFESA será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento. As informações privadas ou confidenciais sob a guarda da AC DEFESA poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

### 9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

### 9.4.8 Informações a terceiros

Nenhum documento, informação ou registro sob a guarda da AC DEFESA, responsável pela DPC, ou sob guarda das ARs a ela vinculadas, deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

## 9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

## 9.6 Declarações e Garantias

### 9.6.1 Declarações e Garantias da AC DEFESA

A AC DEFESA declara e garante o quanto segue:

#### 9.6.1.1 Autorização para certificado

A AC DEFESA implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC DEFESA, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ARs a ela vinculadas na forma de suas DPCs, PCs e normas complementares.

#### 9.6.1.2 Precisão da informação

A AC DEFESA implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes e ARs na forma de suas DPCs, PCs e normas complementares.

**9.6.1.3** Identificação do requerente

A AC DEFESA implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC DEFESA, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ARs a ela vinculadas na forma de suas DPCs, PCs e normas complementares.

**9.6.1.4** Consentimento dos titulares

A AC DEFESA implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

**9.6.1.5** Serviço

A AC mantém 24x7 acesso ao seu repositório com a informação do seu próprio certificado e LCRs.

**9.6.1.6** Revogação

A AC DEFESA irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil.

**9.6.1.7** Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

### 9.6.2 Declarações e Garantias das ARs

Em acordo com item 4 desta DPC.

### 9.6.3 Declarações e garantias do titular

**9.6.3.1** Toda informação necessária para a identificação do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC DEFESA, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

**9.6.3.2** A AC DEFESA deve informar à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

### 9.6.4 Declarações e garantias das terceiras partes

**9.6.4.1** As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;

b) verificar, a qualquer tempo, a validade do certificado.

**9.6.4.2** O certificado da AC é considerado válido quando:

i) tiver sido emitido pela AC;
ii) não constar como revogado pela AC;
iii) não estiver expirado; e
iv) puder ser verificado com o uso do certificado válido da AC.

**9.6.4.3** A utilização ou aceitação de certificados sem a observância das providências descritas é de conta e risco da terceira parte que usar ou aceitar a utilização do respectivo certificado.

### 9.6.5 Representações e garantias de outros participantes

Não se aplica.

## 9.7 Isenção de garantias

Não se aplica.

## 9.8 Limitações de responsabilidades

A AC DEFESA não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

## 9.9 Indenizações

A AC DEFESA responde pelos danos que der causa e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

## 9.10 Prazo e Rescisão

### 9.10.1 Prazo

Esta DPC entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

### 9.10.2 Término

Esta DPC vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

#### 9.10.3 Efeito da rescisão e sobrevivência

Os atos praticados na vigência desta DPC são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

## 9.11 Avisos individuais e comunicações com os participantes

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

## 9.12 Alterações

### 9.12.1 Procedimento para emendas

Qualquer alteração nesta DPC será submetida para aprovação da AC Raiz.

### 9.12.2 Mecanismo de notificação e períodos

Mudanças nesta DPC serão publicadas no site da AC DEFESA, ficando disponível para consulta na área de documentação do ambiente principal e na contingência, acessível pela URL:
*https://www.acdefesa.mil.br/index.php/documentacao*

### 9.12.3 Circunstâncias na qual o OID deve ser alterado

Não se aplica.

## 9.13 Solução de conflitos

**9.13.1** Os litígios decorrentes desta DPC serão solucionados de acordo com a legislação vigente.

**9.13.2** Esta DPC não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

## 9.14 Lei aplicável

Esta DPC é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

## 9.15 Conformidade com a Lei aplicável

A AC DEFESA está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

## 9.16 Disposições Diversas

### 9.16.1 Acordo completo

Esta DPC representa as obrigações e deveres aplicáveis à AC DEFESA e as ARs a ela vinculadas. Havendo conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

### 9.16.2 Cessão

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

### 9.16.3 Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.

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

De acordo com a legislação vigente.

## 9.17 Outras provisões

Não se aplica.

# 10 DOCUMENTOS REFERENCIADOS

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

| Ref. | Nome do documento | Código |
|---|---|---|
| [2] | CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-09 |
| [3] | CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-08 |
| [5] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL | DOC-ICP-17 |
| [6] | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL | DOC-ICP-03 |
| [7] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL | DOC-ICP-04 |
| [8] | POLÍTICA DE SEGURANÇA DA ICP-BRASIL | DOC-ICP-02 |
| [12] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL | DOC-ICP-12 |
| [13] | POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL | DOC-ICP-06 |

**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 sitio *https://www.iti.gov.br* publica a versão mais atualizada desses documentos e as instruções Normativas que os aprovam.

| Ref. | Nome do documento | Código |
|---|---|---|
| [1] | CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL | DOC-ICP-03.01 |
| [9] | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL | DOC-ICP-01.01 |
| [10] | PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL | DOC-ICP-05.02 |
| [11] | PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL | DOC-ICP-05.03 |

**10.3** Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados mediante publicação de uma nova versão no sítio *https://www.iti.gov.br*.

| Ref. | Nome do documento | Código |
|---|---|---|
| [4] | TERMOS DE TITULARIDADE | ADE-ICP-05.B |

# 11 REFERÊNCIAS BIBLIOGRÁFICAS

**[5]** WebTrust Principles and Criteria for Registration Authorities, disponível em *http://www.webtrust.org*.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

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

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

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