**Infraestrutura de Chaves Públicas Brasileira**

# REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL

## DOC-ICP-05 - Versão 3.5

## 18 de novembro de 2010

# Infraestrutura de Chaves Públicas Brasileira

## Sumário

# Infraestrutura de Chaves Públicas Brasileira

*CONTROLE DE ALTERAÇÕES*

***Tabela 1 – Tabela de Controle de Alterações***

| Resolução que aprovou a alteração | Item Alterado | Descrição da Alteração |
|---|---|---|
| **Resolução 84, de 18 de novembro de 2010 (Versão 3.5)** | 2.2.1.3, 3.1.1.6, 3.1.9.1, 3.1.9.2.1, 4.1.1, 4.4.2 | Inclui procedimentos para a emissão de certificados digitais que integram o documento de Registro de Identidade Civil-RIC. |
| **Resolução 79, de 07 de junho de 2010 (Versão 3.4)** | 3.1.1.1 | Complementa os requisitos para procuração de pessoa jurídica, para aceitação apenas quando o ato constitutivo prevê. |
| **Resolução 75, de 31 de março de 2010 (Versão 3.3)** | 4.6.2, 4.4.11 | Altera prazo de retenção do dossiê. |
| **Resolução 74, de 24 de novembro de 2009 (Versão 3.2)** | 2.1.3, 3.1.10.1.3, 3.1.10.3.2 4.1.1, 4.5.1.7, 9.3 | Alterações relacionadas aos procedimentos operacionais para utilização de Termo de Titularidade. |
| **Resolução 66, de 06 de junho de 2009 (Versão 3.1)** | 3.2.2 | Altera procedimentos para a renovação de certificados digitais de Pessoa Jurídica. |

*Continua na próxima página*

*Tabela 1 – Conclusão da Tabela de Controle de Alterações*

| Resolução que aprovou a alteração | Item Alterado | Descrição da Alteração |
|---|---|---|
| **Resolução 54, de 19.11.2008 (Versão 3.0)** | 3.1.11.2.2 , 4.1.3 | Inclusão de referências a Carimbo de Tempo. |
| **Resolução 48, de 03.12.2007 (Versão 2.1)** | 3.1.10.2 | Alterados os documentos a serem apresentados para identificação de uma organização que solicita certificado digital. |
| | 3.1.1.5 | Incluído item sobre identificação de Servidores do Serviço Exterior Brasileiro em missão permanente no exterior. |
| | 6.6.4 | Incluído item exigindo verificação de consistência do conteúdo das LCRs, antes de sua publicação. |
| **Resolução 42, de 18.04.2006 (Versão 2.0)** | Diversos | Criação do DOC-ICP-05, consolidando documentos anteriores |

## *SIGLAS*

***Tabela 2 – Tabela de Siglas***

| SIGLA | DESCRIÇÃO |
|---|---|
| **AC** | Autoridade Certificadora |
| **AC Raiz** | Autoridade Certificadora Raiz da ICP-Brasil |
| **ACT** | Autoridade de Carimbo do Tempo |
| **AR** | Autoridades de Registro |
| **CEI** | Cadastro Específico do INSS |
| **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 |
| **DMZ** | Zona Desmilitarizada |

*Continua na próxima página*

*Tabela 2 – Continuação da Tabela de Siglas*

| SIGLA | DESCRIÇÃO |
|---|---|
| **DN** | *Distinguished Name* |
| **DPC** | Declaração de Práticas de Certificação |
| **ICP-Brasil** | Infraestrutura de Chaves Públicas Brasileira |
| **IDS** | *Intrusion Detection System* |
| **IEC** | *International Electrotechnical Commission* |
| **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* |
| **OID** | *Object Identifier* |
| **OU** | *Organization Unit* |
| **PASEP** | Programa de Formação do Patrimônio do Servidor Público |

*Continua na próxima página*

*Tabela 2 – Conclusão da Tabela de Siglas*

| SIGLA | DESCRIÇÃO |
|---|---|
| **PC** | Política de Certificado |
| **PCN** | Plano de Continuidade de Negócio |
| **PIS** | Programa de Integração Social |
| **POP** | Proof of Possession |
| **PS** | Política de Segurança |
| **PSS** | Prestadores de Serviço de Suporte |
| **RFC** | Request For Comments |
| **RG** | Registro Geral |
| **SINRIC** | Sistema Nacional de Registro de Identificação Civil |
| **SNMP** | Simple Network Management Protocol |
| **TCSEC** | Trusted System Evaluation Criteria |
| **TSDM** | Trusted Software Development Methodology |
| **UF** | Unidade de Federação |
| **URL** | Uniform Resource Locator |

# 1. INTRODUÇÃO

## 1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos mínimos, a serem obrigatoriamente observados pelas Autoridades Certificadoras - AC integrantes da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços .

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

## 1.2. Identificação

Neste item deve ser identificada a DPC e indicado o seu OID (*Object Identifier*). No âmbito da ICP-Brasil, um OID – com o formato 2.16.76.1.1.n – será atribuído à DPC na conclusão do processo de credenciamento da AC responsável.

## 1.3. Comunidade e Aplicabilidade

### 1.3.1. Autoridades Certificadoras

Neste item deve ser identificada a AC integrante da ICP-Brasil a que se refere a DPC.

### 1.3.2. Autoridades de Registro

1.3.2.1. Neste item deve ser identificado o endereço da página *web* (URL) onde estão publicados os dados a seguir, referentes às Autoridades de Registro (ARs) utilizadas pela AC para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes:

a) relação de todas as ARS credenciadas, com informações sobre as PCs que implementam;
b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data de encerramento das atividades;
f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2. A AC responsável deverá manter as informações acima sempre atualizadas.

### 1.3.3. Prestador de Serviços de Suporte

1.3.3.1. Neste item deve ser identificado o endereço da página *web* (URL) onde está publicada a relação de todos os Prestadores de Serviços de Suporte – PSS vinculados à AC responsável, seja diretamente seja por intermédio de suas ARs.

1.3.3.2. PSSs são entidades utilizados pela AC ou pela AR para desempenhar atividade descrita nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

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

1.3.3.3. A AC responsável deverá manter as informações acima sempre atualizadas.

### 1.3.4. Titulares de Certificado

Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão ser titulares dos certificados emitidos segundo a DPC. Quando aplicável, devem ser caracterizadas as ACs subseqüentes para as quais a AC responsável pela DPC poderá emitir certificados.

### 1.3.5. Aplicabilidade

Este item da DPC deve relacionar e identificar as PCs implementadas pela AC responsável, que definem como os certificados emitidos deverão ser utilizados pela comunidade. Nas PCs estarão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

## 1.4. Dados de Contato

Neste item devem ser incluídos nome, endereço e outras informações da AC responsável pela DPC.

Devem ser também informados o nome, os números de telefone e de fax e o endereço eletrônico de uma pessoa para contato.

## 2. DISPOSIÇÕES GERAIS

### 2.1. Obrigações e direitos

Nos itens a seguir devem ser descritas as obrigações gerais das entidades envolvidas. Caso haja obrigações específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

#### 2.1.1. Obrigações da AC

Neste item devem ser incluídas as obrigações da AC responsável pela DPC, contendo, no mínimo, as abaixo relacionadas:

a) operar de acordo com a sua DPC e com as PCs 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 AC de nível imediatamente subseqüente ao seu ou os certificados de AR a ela vinculadas 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 LCRs e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
k) publicar em sua página *web* sua DPC e as PCs aprovadas que implementa;
l) publicar, em sua página *web*, as informações definidas no item 2.6.1.2 deste documento;
m) publicar, em página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica,
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 implementar, 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) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subseqüente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

### 2.1.2. Obrigações das ARs

Neste item devem ser incluídas as obrigações das ARs vinculadas à AC responsável pela DPC, contendo, no mínimo, as abaixo relacionadas:

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;
f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];

h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
i) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
j) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas.

### 2.1.3. Obrigações do Titular do Certificado

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos pela AC responsável pela DPC, constantes dos termos de titularidade de que trata o item 4.1.1, devendo incluir no mínimo os itens 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, senhas 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 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.

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

### 2.1.4. Direitos da terceira parte (*Relying Party*)

2.1.4.1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2. Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
   i. não constar da LCR da AC emitente;
   ii. não estiver expirado; e

iii. puder ser verificado com o uso de certificado válido da AC emitente.

2.1.4.3. O não exercício desses direitos não afasta a responsabilidade da AC responsável e do titular do certificado.

### 2.1.5. Obrigações do Repositório

Em caso de uso de repositório, neste item devem ser incluídas as obrigações do mesmo, entre elas:

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e a sua 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.

## 2.2. Responsabilidades

### 2.2.1. Responsabilidades da AC

2.2.1.1. A AC responsável responde pelos danos a que der causa.

2.2.1.2. A AC responde solidariamente pelos atos das entidades de sua cadeia de certificação: AC subordinadas, AR e PSS.

2.2.1.3. Quando da emissão de certificado que integra o Documento RIC, as entidades integrantes da ICP-Brasil não possuirão qualquer espécie de responsabilidade por eventuais danos gerados na identificação presencial do cidadão, a cargo do Estado ( CF / 88 , art. 37 & 6 ).

### 2.2.2. Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

## 2.3. Responsabilidade Financeira

### 2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)

Neste item deve ser estabelecida a inexistência de responsabilidade da terceira parte (*Relying Party*) perante a AC ou AR a ela vinculada, exceto na hipótese de prática de ato ilícito.

### 2.3.2. Relações Fiduciárias

Neste item deve constar que a AC responsável ou AR vinculada indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

### 2.3.3. Processos Administrativos

Neste item devem ser relacionados os processos administrativos cabíveis, relativos às operações da AC responsável pela DPC e das ARs vinculadas.

## 2.4. Interpretação e Execução

### 2.4.1. Legislação

Neste item deve ser indicada a legislação que ampara a DPC.

### 2.4.2. Forma de interpretação e notificação

2.4.2.1. Neste item devem ser relacionadas as providências a serem tomadas na hipótese de uma ou mais das disposições da DPC ser, por qualquer razão, considerada inválida, ilegal ou não aplicável.

2.4.2.2. Deve também ser definida a forma pela qual serão realizadas as notificações, as solicitações ou quaisquer outras comunicações necessárias, relativas às práticas descritas na DPC.

### 2.4.3. Procedimentos de solução de disputa

2.4.3.1. Neste item devem ser definidos os procedimentos a serem adotados em caso de conflito entre a DPC e outras declarações, políticas, planos, acordos, contratos ou documentos que a AC adotar.

2.4.3.2. Deve também ser estabelecido que a DPC da AC responsável não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3. Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

### 2.5. Tarifas de Serviço

Nos itens a seguir, devem ser especificadas pela AC responsável pela DPC as políticas tarifária e de reembolso aplicáveis. Caso sejam aplicadas tarifas específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

2.5.1. Tarifas de emissão e renovação de certificados
2.5.2. Tarifas de acesso ao certificado
2.5.3. Tarifas de revogação ou de acesso à informação de status
2.5.4. Tarifas para outros serviços
2.5.5. Política de reembolso

### 2.6. Publicação e Repositório

#### 2.6.1. Publicação de informação da AC

2.6.1.1. Neste item devem ser definidas as informações a serem publicadas pela AC responsável pela DPC, o modo pelo qual serão disponibilizadas e a sua disponibilidade, que deverá ser, no mínimo, de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações, no mínimo, deverão ser publicadas pela AC em serviço de diretório ou página *web*:

a) seu próprio certificado;
b) suas LCRs;
c) sua DPC;
d) as PCs que implementa;
e) uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
f) uma relação, regularmente atualizada, das ARs vinculadas que tenham celebrado acordos operacionais com outras ARs da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e
g) uma relação, regularmente atualizada, dos PSSs vinculados.

### 2.6.2. Freqüência de publicação

Neste item deve ser informada a freqüência de publicação das informações de que trata o item anterior, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

### 2.6.3. Controles de acesso

Neste item devem ser descritos os controles e as eventuais restrições para acesso, leitura e escrita das informações publicadas pela AC, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil.

### 2.6.4. Repositórios

Neste item devem ser descritos os requisitos aplicáveis aos repositórios utilizados pela AC responsável pela DPC, tais como:

a) localização lógica;
b) disponibilidade;
c) protocolos de acesso; e
d) requisitos de segurança.

## 2.7. Fiscalização e Auditoria de Conformidade

2.7.1. 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.

2.7.2. 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].
2.7.3. 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].

2.7.4. Neste item da DPC, a AC responsável deve informar que recebeu auditoria prévia da AC Raiz

para fins de credenciamento na ICP-Brasil e que é 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, freqüência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. Neste item da DPC, a AR responsável deve informar que as entidades da ICP-Brasil a ela diretamente vinculadas (AC, AR e PSS), também receberam auditoria prévia, para fins de credenciamento, e que a AC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

### 2.8. Sigilo

#### 2.8.1. Disposições Gerais

2.8.1.1. A chave privada de assinatura digital da AC credenciada responsável pela DPC será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.

2.8.1.2. A DPC deve informar 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. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3. No caso de certificados de sigilo emitidos pela AC, a DPC deve delimitar as responsabilidades pela manutenção e pela garantia do sigilo das respectivas chaves privadas. Caso existam responsabilidades específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

#### 2.8.2. Tipos de informações sigilosas

2.8.2.1. Neste item devem ser identificados os tipos de informações consideradas sigilosas pela AC responsável pela DPC e pelas ARs a ela vinculadas, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.8.2.2. A DPC deve estabelecer, como princípio geral, que nenhum documento, informação ou registro fornecido à AC ou às ARs vinculadas deverá ser divulgado.

### 2.8.3. Tipos de informações não sigilosas

Neste item devem ser indicados os tipos de informações consideradas não sigilosas pela AC responsável pela DPC e pelas ARs a ela vinculadas, os quais deverão compreender, entre outros:

a) os certificados e as LCRs emitidos pela AC;
b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
c) as PCs implementadas pela AC;
d) a DPC da AC;
e) versões públicas de PS; e
f) a conclusão dos relatórios de auditoria.

### 2.8.4. Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. Neste item devem ser descritas as formas previstas pela AC responsável pela DPC para a divulgação de informação de revogação dos certificados por ela emitidos. O item deve informar também a política adotada pela AC para a divulgação ou não divulgação das razões para a revogação dos certificados para terceiros.

2.8.4.2. As razões para revogação do certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

2.8.4.3. A DPC deve ainda informar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

### 2.8.5. Quebra de sigilo por motivos legais

Este item deve estabelecer o dever da AC responsável pela DPC de fornecer documentos, informações ou registros sob sua guarda, mediante ordem judicial.

### 2.8.6. Informações a terceiros

Este item da DPC deve estabelecer como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC responsável pela DPC 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.

**2.8.7. Divulgação por solicitação do titular**

2.8.7.1. Neste item devem ser descritas as condições sob as quais um titular de certificado ou seu representante legal, poderá ter acesso a quaisquer dos seus dados ou identificações, ou poderá autorizar a divulgação de seus registros a outras pessoas.

2.8.7.2. A DPC deve estabelecer que qualquer liberação de informação pela AC responsável ou pelas ARs vinculadas somente será permitida mediante autorização formal do titular do certificado. As formas de apresentação dessa autorização devem ser definidas pela DPC.

**2.8.8. Outras circunstâncias de divulgação de informação**

Neste item da DPC devem ser descritas, quando cabíveis, quaisquer outras circunstâncias em que poderão ser divulgadas informações sigilosas.

**2.9. Direitos de Propriedade Intelectual**

Neste item da DPC devem ser tratadas as questões referentes aos direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, de acordo com a legislação vigente.

## 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

### 3.1. Registro Inicial

#### 3.1.1. Disposições Gerais

3.1.1.1 Neste item e nos seguintes, a DPC deve descrever em detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas à AC responsável para realização dos seguintes processos:

a) Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:
   i. confirmação da identidade de um individuo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados

constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil.

ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

iii. 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;

b) Verificação da solicitação de certificado - confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

i. por agente de registro distinto do que executou a etapa de validação;

ii. em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

iii. somente após o recebimento, na instalação técnica da AR, de cópia dos da documentação apresentada na etapa de validação;

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

3.1.1.2. O processo de validação poderá ser realizado pelo agente de registro fora do ambiente físico da AR, desde que utilizado ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. Tais registros devem feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.1.1.5. 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 subitem 3.1.1.1 deste anexo, 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.

3.1.1.6. Disposições para a Validação de Solicitação de Certificados que integram Documentos RIC: A solicitação de certificado que integra o Documento RIC, realizada por Órgão de Identificação integrante do SINRIC, conforme LEI 12.058 de 13 de outubro de 2009, deverá:

a) realizar a validação do registro inicial por meio de processo de individualização unívoca do cidadão com a consequente atribuição de número RIC, conforme as Leis 9454, de 07 de abril de 1997, 12.058 de 13 de outubro de 2009 e Decreto 7.166, de 05 de maio de 2010, bem como demais resoluções do Comitê-Gestor do Registro de Identidade Civil – CG-RIC;
b) realizar a verificação da solicitação de certificado mediante autenticação biométrica automatizada da pessoa que se apresenta como titular do certificado de pessoa física, feita na presença de funcionário do Orgão de Identificação, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC;
c) obter os dados, enviados para que a AC emita o certificado digital, da memória do Cartão RIC, sem que haja possibilidade de alteração destes por parte do agente de AR, após autenticação biométrica utilizando os recursos do Cartão RIC (*match-on-card*).

### 3.1.2. Tipos de nomes

3.1.2.1. Neste item, devem ser definidos os tipos de nomes admitidos para os titulares de certificados emitidos pela AC responsável pela DPC. Entre os tipos de nomes considerados, poderão estar o "*distinguished name"* do padrão ITU X.500, endereços de correio eletrônico ou endereços de página *web* (URL).

3.1.2.2. A DPC deve estabelecer, ainda, que um certificado emitido para uma AC subseqüente não deverá incluir o nome da pessoa responsável.

### 3.1.3. Necessidade de nomes significativos

Neste item, a DPC deve definir a necessidade do uso de nomes significativos, isto é, nomes que possibilitem determinar a identidade da pessoa ou organização a que se referem, para a identificação dos titulares dos certificados emitidos pela AC responsável.

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

Neste item devem ser descritas, quando aplicáveis, as regras para a interpretação das várias formas de nomes admitidas pela DPC.

### 3.1.5. Unicidade de nomes

Neste item, a DPC deve estabelecer que identificadores do tipo "*Distinguished Name*" (DN) deverão ser únicos para cada titular de certificado, no âmbito da AC emitente. 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

Neste item, a DPC deve reservar à AC responsável o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes diversos de certificados. Deve estabelecer também que, 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

Neste item a DPC deve estabelecer que os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

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

A DPC deve indicar os procedimentos executados pela AC responsável ou pelas ARs a ela vinculadas para confirmar que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, podendo utilizar para isso as referências contidas na RFC 2510, relativos a POP (*Proof of Possession*). Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

### 3.1.9. Autenticação da identidade de um indivíduo

Neste item devem ser definidos os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos.

### 3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de um indivíduo solicitante de certificado:

a) Cédula de Identidade ou Passaporte, se brasileiro;
b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
c) Passaporte, se estrangeiro não domiciliado no Brasil;
d) Caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;
e) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e
f) Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4.

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 4: Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

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

3.1.9.2.1. 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]
b) data de nascimento.[2]
c) número RIC, quando da emissão de certificado que integra Documento RIC.

1 No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*
2 No campo *Subject Alternative Name*, nas primeiras 8 (oito) posições do **OID 2.16.76.1.3.1**

3.1.9.2.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

a) Cadastro de Pessoa Física (CPF);
b) número de Identificação Social - NIS (PIS, PASEP ou CI);
c) número do Registro Geral - RG do titular e órgão expedidor;
d) número do Cadastro Especifico do INSS (CEI);
e) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.1.9.2.3. Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original. Deve ser mantido 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.

### 3.1.10. Autenticação da identidade de uma organização

#### 3.1.10.1. Disposições Gerais

3.1.10.1.1. Neste item devem ser definidos os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica.

3.1.10.1.2. Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

3.1.10.1.3. Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;
b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is)

da pessoa jurídica e do responsável pelo uso do certificado;
c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.

### 3.1.10.2. 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 a 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:
      1. ato constitutivo, devidamente registrado no órgão competente; e
      2. documentos da eleição de seus administradores, quando aplicável;
b) Relativos a 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.

### 3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. 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]

3.1.10.3.2. 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 3.1.9.2.

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**

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

#### 3.1.11.1. Disposições Gerais

3.1.11.1.1. Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

3.1.11.1.2. Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.1.9.1. e esta assinará o termo de titularidade de que trata o item 4.1.1.

3.1.11.1.3. Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) Apresentação do rol de documentos elencados no item 3.1.10.2;
b) Apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) Presença física do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e
d) Presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade de que trata o item 4.1.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

#### 3.1.11.2. Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.1.11.2.1. Para certificados de equipamento ou aplicação que utilizem URL no campo *Common Name*, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele nome. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

3.1.11.2.2. Para emissão de certificados do tipo T3 ou T4, para equipamentos de ACT credenciadas na ICP-Brasil, a solicitação deve conter o nome de servidor e o número de série do equipamento. Esses dados devem ser validados comparando-os com aqueles publicados pelo ITI no Diário Oficial da União, quando do deferimento do credenciamento da ACT.

### 3.1.11.3. Informações contidas no certificado emitido para um equipamento ou aplicação

3.1.11.3.1. É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nos documentos apresentados:

a) URL ou nome da aplicação;[1]
b) nome completo do responsável pelo certificado, sem abreviações;[2]
c) data de nascimento do responsável pelo certificado;[3]
d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[4], se o titular for pessoa jurídica;
e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[5], se o titular for pessoa jurídica.

3.1.11.3.2. 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 responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

## 3.2. Geração de novo par de chaves antes da expiração do atual

3.2.1. Neste item a DPC deve estabelecer os processos de identificação do solicitante utilizados pela AC responsável para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.2.2. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

a) Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
b) A solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva;
c) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

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

1 No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*
2 No campo *Subject Alternative Name*, OID **2.16.76.1.3.2**
3 No campo *Subject Alternative Name*, nas primeiras 8 (oito) posições do OID **2.16.76.1.3.4**
4 No campo *Subject Alternative Name*, *OID **2.16.76.1.3.8***
5 No campo *Subject Alternative Name*, OID **2.16.76.1.3.3**

### 3.3. Geração de novo par de chaves após expiração ou revogação

3.3.1. Neste item, a DPC deve descrever os procedimentos utilizados para confirmação da identidade de uma entidade solicitante de novo certificado, após a expiração ou revogação do certificado dessa entidade. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

3.3.2. Para o caso específico de revogação de um certificado de AC de nível imediatamente subseqüente ao da AC responsável pela DPC, este item deve estabelecer que, após a expiração ou revogação de seu certificado, aquela AC deverá executar os processos regulares de geração de seu novo par de chaves.

### 3.4. Solicitação de Revogação

Neste item, a DPC deve descrever os procedimentos utilizados para a confirmação da identidade do solicitante de uma revogação de certificado. A DPC deve exigir que solicitações de revogação de certificado sejam sempre registradas. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

## 4. REQUISITOS OPERACIONAIS

### 4.1. Solicitação de Certificado

4.1.1. Neste item da DPC devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável e pelas ARs a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos deverão compreender, no mínimo:

a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
b) mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de tipo A3, a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados, ou quando da emissão de certificado que integra Documento RIC, de funcionário de Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009; e
c) um termo de titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, no caso de pessoa jurídica, conforme o adendo referente ao TERMO DE

TITULARIDADE [4] específico, ou, quando da emissão de certificado que integra Documento RIC, um Guia Informativo entregue ao titular do certificado.

4.1.2. A DPC deve observar, quando aplicável, que a solicitação de certificado para AC de nível imediatamente subseqüente ao da AC responsável somente será possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. A DPC deve observar, quando aplicável, que a solicitação de certificado para equipamento de carimbo do tempo de Autoridade de Carimbo do Tempo (ACT) credenciada na ICP-Brasil somente será possível após o processo de credenciamento e a autorização de funcionamento da ACT em questão, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.4. Nos casos previstos no item 4.1.2., a AC subseqüente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

**4.2. Emissão de Certificado**

4.2.1. Neste item da DPC devem ser descritos os requisitos operacionais estabelecidos pela AC para a emissão de certificado e para a notificação da emissão à entidade solicitante. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

4.2.2. A DPC deve observar que um certificado será considerado válido a partir do momento de sua emissão.

**4.3. Aceitação de Certificado**

4.3.1. Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à aceitação de um certificado por seu titular. Devem ser apontadas as implicações decorrentes dessa aceitação, ou não aceitação. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

4.3.2. A DPC deve garantir que a aceitação de todo certificado emitido seja declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou

aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.3.3. Eventuais termos de acordo, ou instrumentos similares, requeridos devem ser descritos neste item da DPC.

### 4.4. Suspensão e Revogação de Certificado

#### 4.4.1. Circunstâncias para revogação

4.4.1.1. Neste item da DPC, devem ser caracterizadas as circunstâncias nas quais um certificado poderá ser revogado.

4.4.1.2. Este item deve também estabelecer que um certificado deverá obrigatoriamente ser revogado:

a) Quando constatada emissão imprópria ou defeituosa do mesmo;
b) Quando for necessária a alteração de qualquer informação constante no mesmo;
c) No caso de dissolução de AC titular do certificado; ou
d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.4.1.3. A DPC deve observar ainda que:

a) A AC emitente deverá revogar, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
b) O CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

#### 4.4.2. Quem pode solicitar revogação

A DPC deve estabelecer que a revogação de um certificado somente poderá ser feita:

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC emitente;

e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
g) Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009, quando tratar-se de certificado que integra Documento RIC emitido pelo respectivo Orgão.

### 4.4.3. Procedimento para solicitação de revogação

4.4.3.1 Neste item da DPC devem ser descritos os procedimentos estabelecidos pela AC para a solicitação de revogação de certificados. A AC deverá garantir que todos agentes habilitados, conforme o item 4.4.2., possam, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

4.4.3.2. Como diretrizes gerais, a DPC deve estabelecer que:

a) O solicitante da revogação de um certificado será identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;
c) As justificativas para a revogação de um certificado serão documentadas; e
d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

4.4.3.3 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 12 (doze) horas.

4.4.3.4. O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 12 (doze) horas.

4.4.3.5 A DPC deve garantir que a AC responsável 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.

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

### 4.4.4. Prazo para solicitação de revogação

4.4.4.1 Neste item, a DPC deve observar que a solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no seu item 4.4.1 e deve estabelecer o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado poderá ser solicitada sem cobrança de tarifa pela AC.

4.4.4.2 Caso sejam requeridos prazos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

### 4.4.5. Circunstâncias para suspensão

A DPC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

### 4.4.6. Quem pode solicitar suspensão

A DPC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

### 4.4.7. Procedimento para solicitação de suspensão

A DPC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

### 4.4.8. Limites no período de suspensão

A DPC deve observar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil.

### 4.4.9. Freqüência de emissão de LCR

4.4.9.1. Neste item deve ser definida a freqüência de emissão da LCR referente a certificados de usuários finais e de AC de nível imediatamente subseqüente ao da AC responsável.

4.4.9.2. A freqüência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 horas.

4.4.9.3. A freqüência máxima admitida para a emissão de LCR referente a certificados de AC é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC responsável deverá emitir nova LCR no prazo previsto no item 4.4.3 e notificar todas as ACs de nível imediatamente subseqüente ao seu.

4.4.9.4. Caso sejam utilizadas freqüências de emissão de LCR específicas para as PCs implementadas, as mesmas devem ser descritas nessas PCs, no item correspondente.

**4.4.10. Requisitos para verificação de LCR**

4.4.10.1. Neste item, a DPC deve observar que todo certificado deverá ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.4.10.2 A DPC deve observar ainda, que a autenticidade da LCR deverá também ser confirmada, por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

**4.4.11. Disponibilidade para revogação ou verificação de status *on-line***

Neste item, a DPC deve informar, se for o caso, as disponibilidades de recursos da AC responsável para revogação *on-line* de certificados ou para verificação *on-line* de *status* de certificados. A verificação da situação de um certificado deverá ser feita diretamente na AC emitente, por meio do protocolo OCSP (*On-line Certificate Status Protocol*).

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

Neste item, a DPC deve definir, quando cabíveis, os requisitos para a verificação *on-lin*e de informações de revogação de certificados por parte das terceiras partes (*relying parties*). Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

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

Neste item, a DPC deve informar, quando existirem, outras formas utilizadas pela AC responsável para a divulgação de informações de revogação de certificados.

**4.4.14. Requisitos para verificação de outras formas de divulgação de revogação**

Neste item, a DPC deve definir, quando cabíveis, os requisitos para a verificação das formas de divulgação indicadas no item anterior e de informações de revogação de certificados, pelas terceiras partes (*relying parties*).

### 4.4.15. Requisitos especiais para o caso de comprometimento de chave

4.4.15.1. Neste item da DPC devem ser definidos os requisitos aplicáveis à revogação de certificado provocada pelo comprometimento da chave privada correspondente. A DPC deve observar que, nessa circunstância, o titular do certificado deverá comunicar o fato imediatamente à AC emitente. Caso haja requisitos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

4.4.15.2 A DPC deve conter também determinações que definam os meios utilizados para comunicar um comprometimento ou suspeita de comprometimento de chave.

## 4.5. Procedimentos de Auditoria de Segurança

Nos itens seguintes da DPC devem ser descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC responsável com o objetivo de manter um ambiente seguro.

### 4.5.1. Tipos de eventos registrados

4.5.1.1. A AC responsável pela DPC deverá registrar em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
c) Mudanças na configuração da AC 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 ou de chaves de seus usuários finais;
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; e
l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2. A AC responsável pela DPC deverá também registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

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.

4.5.1.3. Neste item, a DPC deve especificar todas as informações que deverão ser registradas pela AC responsável.

4.5.1.4. A DPC deve prever que todos os registros de auditoria, eletrônicos ou manuais, deverão conter a data e a hora do evento registrado e a identidade do agente que o causou.

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

4.5.1.6. A AR vinculada à AC responsável pela DPC deverá registrar eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) Os agentes de registro que realizaram as operações;
b) Data e hora das operações;
c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;
d) A assinatura digital do executante.

4.5.1.7. A AC a que esteja vinculada a AR deve definir, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados, e dos termos de titularidade.

### 4.5.2. Freqüência de auditoria de registros (*logs*)

A DPC deve estabelecer a periodicidade, não superior a uma semana, com que os registros de auditoria da AC responsável serão analisados pelo seu pessoal operacional. Todos os eventos

significativos deverão ser explicados em relatório de auditoria de registros. Tal análise deverá envolver uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise deverão ser documentadas.

### 4.5.3. Período de retenção para registros (*logs*) de auditoria

Neste item, a DPC deve estabelecer que a AC responsável manterá localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, deverá armazená-los da maneira descrita no item 4.6.

### 4.5.4. Proteção de registro (*log*) de auditoria

4.5.4.1. Neste item, a DPC deve descrever os mecanismos obrigatórios incluídos no sistema de registro de eventos da AC responsável para proteger os seus registros de auditoria contra leitura não autorizada, modificação e remoção.

4.5.4.2. Também devem ser descritos os mecanismos obrigatórios de proteção de informações manuais de auditoria contra a leitura não autorizada, modificação e remoção.

4.5.4.3. Os mecanismos de proteção descritos neste item devem obedecer à POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

### 4.5.5. Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

Neste item da DPC devem ser descritos os procedimentos adotados pela AC responsável para gerar cópias de segurança (*backup*) de seus registros de auditoria e a sua periodicidade, que não deve ser superior a uma semana.

### 4.5.6. Sistema de coleta de dados de auditoria

Neste item da DPC devem ser descritos e localizados os recursos utilizados pela AC responsável para a coleta de dados de auditoria.

### 4.5.7. Notificação de agentes causadores de eventos

A DPC deve observar que quando um evento for registrado pelo conjunto de sistemas de auditoria da AC responsável, nenhuma notificação deverá ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

### 4.5.8. Avaliações de vulnerabilidade

A DPC deve assegurar que os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC responsável, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes deverão ser implementadas pela AC e registradas para fins de auditoria.

## 4.6. Arquivamento de Registros

Nos itens seguintes da DPC deve ser descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC responsável e pelas ARs a ela vinculadas.

### 4.6.1. Tipos de registros arquivados

Neste item da DPC devem ser especificados os tipos de registros arquivados, que deverão compreender, entre outros:

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 responsável; e
g) Informações de auditoria previstas no item 4.5.1.

### 4.6.2. Período de retenção para arquivo

Neste item, a DPC deve estabelecer os períodos de retenção para cada registro arquivado, observando que:

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
b) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado. **As prescrições já em curso, quando da alteração desta alínea, terão seu prazo reiniciado;** e
c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no

mínimo, 6 (seis) anos.

**4.6.3. Proteção de arquivo**

A DPC deve estabelecer que todos os registros arquivados deverão ser classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

**4.6.4. Procedimentos para cópia de segurança (*backup*) de arquivo**

4.6.4.1. A DPC deve estabelecer que uma segunda cópia de todo o material arquivado deverá ser armazenada em local externo à AC responsável, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

4.6.4.2. As cópias de segurança deverão seguir os períodos de retenção definidos para os registros dos quais são cópias.

4.6.4.3. A AC responsável pela DPC deverá verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

**4.6.5. Requisitos para datação de registros**

Neste item, a DPC deve estabelecer os formatos e padrões de data e hora contidos em cada tipo de registro.

**4.6.6. Sistema de coleta de dados de arquivo**

Neste item da DPC devem ser descritos e localizados os recursos de coleta de dados de arquivo utilizados pela AC responsável.

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

Neste item da DPC devem ser detalhadamente descritos os procedimentos definidos pela AC responsável e pelas ARs vinculadas para a obtenção ou a verificação de suas informações de arquivo.

**4.7. Troca de chave**

4.7.1. Neste item, a DPC deve descrever os procedimentos para o fornecimento, pela AC

responsável, de um novo certificado, antes da expiração do certificado ainda válido do mesmo titular e definir o prazo anterior à data de expiração do certificado, no qual a AC ou uma AR vinculada comunicará ao seu titular para que seja solicitada a emissão de um novo certificado.

4.7.2. Caso sejam requeridos procedimentos ou prazos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

### 4.8. Comprometimento e Recuperação de Desastre

Nos itens seguintes da DPC devem ser descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC responsável, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

#### 4.8.1. Recursos computacionais, software, e dados corrompidos

Neste item da DPC devem ser descritos os procedimentos de recuperação utilizados pela AC responsável quando recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção.

#### 4.8.2. Certificado de entidade é revogado

Neste item da DPC devem ser descritos os procedimentos de recuperação utilizados na circunstância de revogação do certificado da AC responsável.

#### 4.8.3. Chave de entidade é comprometida

Neste item da DPC devem ser descritos os procedimentos de recuperação utilizados na circunstância de comprometimento da chave privada da AC responsável.

#### 4.8.4. Segurança dos recursos após desastre natural ou de outra natureza

Neste item da DPC devem ser descritos os procedimentos de recuperação utilizados pela AC responsável após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

### 4.8.5. Atividades das Autoridades de Registro

Neste item da DPC devem ser descritos os procedimentos previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;
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 deve ser dada à avaliação da 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;
f) Teste e atualização dos planos.

### 4.9. Extinção dos serviços de AC, AR ou PSS

4.9.1. Observado o disposto no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], este item da DPC deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da AC responsável ou de uma AR ou PSS a ela vinculados.

4.9.2. Devem ser detalhados os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo.

## 5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes devem ser descritos os controles de segurança implementados pela AC responsável pela DPC e pelas ARs a ela vinculadas para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

### 5.1. Controles Físicos

Nos itens seguintes da DPC devem ser descritos os controles físicos referentes às instalações que abrigam os sistemas da AC responsável e das ARs vinculadas.

### 5.1.1. Construção e localização das instalações de AC

5.1.1.1. A DPC deve estabelecer que a localização e o sistema de certificação da AC responsável não deverão ser publicamente identificados. Não deverá haver identificação pública externa das instalações e, internamente, não deverão ser admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações deverão ser segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Neste item, a DPC deve ainda descrever aspectos de construção das instalações da AC responsável, relevantes para os controles de segurança física, compreendendo entre outros:

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas; e
d) Iluminação de emergência.

### 5.1.2. Acesso físico nas instalações de AC

Toda AC integrante da ICP-Brasil deverá implantar um sistema de controle de acesso físico que garanta a segurança de suas instalações, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e os requisitos que seguem.

#### 5.1.2.1. Níveis de acesso

5.1.2.1.1. A DPC deve definir pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC responsável, e mais 2 (dois) níveis relativos à proteção da chave privada da AC.

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

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, terão sua entrada controlada e somente poderão ser

utilizados mediante autorização formal e supervisão.

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

5.1.2.1.5. O terceiro nível – ou nível 3 – deverá situar-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis da operação da AC. Qualquer atividade relativa ao ciclo de vida dos certificados digitais deverá estar localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não deverão ter permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não poderão permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No terceiro nível deverão ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle deverão ser requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

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

5.1.2.1.8. No quarto nível – ou nível 4 -, interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação da AC, tais como a emissão e revogação de certificados e a emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades deverão estar localizados a partir desse nível. O nível 4 deverá possuir os mesmos controles de acesso do nível 3 e, adicionalmente, deverá exigir, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9 No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, 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 deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - deverão possuir proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis.

Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. Poderão existir, na AC, vários ambientes de quarto nível para abrigar e segregar, quando for o caso:

a) Equipamentos de produção *on-line* e cofre de armazenamento;
b) Equipamentos de produção *off-line* e cofre de armazenamento; e
c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

5.1.2.1.12. O quinto nível – ou nível 5 -, interior aos ambientes de nível 4, deverá compreender um cofre ou um gabinete reforçado trancado. Materiais criptográficos, tais como, chaves, dados de ativação, suas cópias e equipamentos criptográficos deverão ser armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre ou o gabinete deverão obedecer às seguintes especificações mínimas:

a) Ser feito em aço ou material de resistência equivalente; e
b) Possuir tranca com chave.

5.1.2.1.14 O sexto nível – ou nível 6 - deverá consistir de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos deverá dispor de fechadura individual. Os dados de ativação da chave privada da AC deverão ser armazenados nesses depósitos.

**5.1.2.2. Sistemas físicos de detecção**

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 1 (um) ano. Elas deverão ser testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas deverão ser 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 deverão ser monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros

separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

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

5.1.2.2.5 O sistema de notificação de alarmes deverá utilizar pelo menos 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, deverão ser permanentemente monitorados por guarda armado e estar localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, deverão ser monitoradas por câmeras de vídeo cujo posicionamento deverá permitir o acompanhamento das ações do guarda.

**5.1.2.3. Sistema de controle de acesso**

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

**5.1.2.4. Mecanismos de emergência**

5.1.2.4.1. Mecanismos específicos deverão ser implantados pela AC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir 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 deve acionar imediatamente os alarmes de abertura de portas.

5.1.2.4.2. A AC poderá especificar e implantar outros mecanismos de emergência, específicos e necessários para cada tipo de instalação. Todos os procedimentos referentes aos mecanismos de emergência deverão ser documentados. Os mecanismos e procedimentos de emergência deverão ser verificados semestralmente, por meio de simulação de situações de emergência.

**5.1.3. Energia e ar condicionado nas instalações de AC**

5.1.3.1. A infraestrutura do ambiente de certificação da AC deverá ser dimensionada com sistemas e dispositivos que garantam o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia devem ser mantidas de forma a atender os requisitos de

disponibilidade dos sistemas da AC e seus respectivos serviços. Um sistema de aterramento deverá ser implantado.

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

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

5.1.3.4. Todos os cabos deverão ser 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. Deverão ser 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 deverá ser previamente documentada.

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

5.1.3.7. O sistema de climatização deverá atender aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispor de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização deverá ser independente e tolerante a falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização deverá ser permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 deverá ser 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 deverá ser 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 nas instalações de AC

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

### 5.1.5. Prevenção e proteção contra incêndio nas instalações de AC

5.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, deverão possibilitar alarmes preventivos antes de fumaça visível, disparados somente 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 não será permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala-cofre de nível 4 deverá possuir sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre deverão constituir eclusas, onde uma porta só deverá se abrir quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC, o aumento da temperatura interna da sala-cofre de nível 4, não deverá exceder 50 graus Celsius, e a sala deverá suportar esta condição por, no mínimo, 1 (uma) hora.

### 5.1.6. Armazenamento de mídia nas instalações de AC

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

### 5.1.7. Destruição de lixo nas instalações de AC

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser 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, deverão ser fisicamente destruídos.

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

As instalações de *backup* deverão atender aos requisitos mínimos estabelecidos por este documento. Sua localização deverá ser tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de *backup* não sejam atingidas e tornem-se totalmente operacionais em condições idênticas em, no máximo, 48 (quarenta e oito) horas.

### 5.1.9. Instalações técnicas de AR

As instalações técnicas de AR deverão atender aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

## 5.2. Controles Procedimentais

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

### 5.2.1. Perfis qualificados

5.2.1.1. A AC responsável pela DPC deverá garantir a separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize indevidamente o seu sistema de certificação sem ser detectado. As ações de cada empregado deverão estar limitadas de acordo com seu perfil.

5.2.1.2. A AC deverá estabelecer 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 deverão receber treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso serão determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4. Quando um empregado se desligar da AC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes 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. A DPC deve estabelecer o requisito de controle multiusuário para a geração e a utilização da chave privada da AC responsável, na forma definida no item 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde estiver localizado o equipamento de certificação da AC deverão requerer a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC poderão ser executadas por um único empregado.

### 5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. A DPC deve garantir que todo empregado da AC responsável terá sua identidade e perfil verificados antes de:

a) Ser incluído em uma lista de acesso às instalações da AC;
b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC;
c) Receber um certificado para executar suas atividades operacionais na AC; e
d) Receber uma conta no sistema de certificação da AC.

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos empregados deverão:

a) Ser diretamente atribuídos a um único empregado;
b) Não ser compartilhados; e
c) Ser restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC deverá implementar um padrão de utilização de "senhas fortes", definido na sua PS e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], juntamente com procedimentos de validação dessas senhas.

## 5.3. Controles de Pessoal

Nos itens seguintes da DPC devem ser descritos requisitos e procedimentos, implementados pela AC responsável, pelas ARs e PSSs 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. A DPC deve garantir que todos os empregados da AC responsável e das ARs e PSSs vinculados, encarregados de tarefas operacionais terão registrado em contrato ou

termo de responsabilidade:

a) Os termos e as condições do perfil que ocuparão;
b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
c) 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 responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC responsável poderá definir requisitos adicionais para a admissão.

### 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 responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser submetido a:

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 responsável poderá definir requisitos adicionais para a verificação de antecedentes.

### 5.3.3. Requisitos de treinamento

Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá receber treinamento documentado, suficiente para o domínio dos seguintes temas:

a) Princípios e mecanismos de segurança da AC e das ARs vinculadas;
b) Sistema de certificação em uso na AC;
c) Procedimentos de recuperação de desastres e de continuidade do negócio;
d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item

3.1.9 e 3.1.10 e 3.1.11; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

### 5.3.4. Freqüência e requisitos para reciclagem técnica

Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC ou das ARs.

### 5.3.5. Freqüência e seqüência de rodízio de cargos

Neste item, a DPC pode definir uma política a ser adotada pela AC responsável e pelas ARs vinculadas para o rodízio de pessoal entre os diversos cargos e perfis por elas estabelecidos. Essa política não deverá contrariar os propósitos estabelecidos no item 5.2.1 para a definição de perfis qualificados.

### 5.3.6. Sanções para ações não autorizadas

5.3.6.1. A DPC deve prever que na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC responsável ou de uma AR vinculada, a AC deverá, de imediato, suspender o acesso dessa pessoa ao seu sistema de certificação, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

5.3.6.2. O processo administrativo referido acima deverá conter, no mínimo, os seguintes itens:

a) Relato da ocorrência com "*modus operandis*";
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 responsável deverá encaminhar 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 contratação de pessoal

Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. A AC responsável poderá definir requisitos adicionais para a contratação.

### 5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A DPC deve garantir que a AC responsável tornará disponível para todo o seu pessoal e para o pessoal das ARs vinculadas, pelo menos:

a) Sua DPC;
b) As PCs que implementa;
c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8];
d) Documentação operacional relativa a suas atividades; e
e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal deverá estar classificada segundo a política de classificação de informação definida pela AC e deverá ser mantida atualizada.

## 6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPC deve definir as medidas de segurança implantadas pela AC responsável para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. Devem também ser definidos outros controles técnicos de segurança utilizados pela AC e pelas ARs vinculadas na execução de suas funções operacionais.

### 6.1. Geração e Instalação do Par de Chaves

### 6.1.1. Geração do par de chaves

6.1.1.1. Neste item, a DPC deve descrever os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da AC responsável. O par de chaves criptográficas da AC

responsável pela DPC deverá ser gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. A DPC deve descrever também os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas de entidade solicitante de certificado. Pares de chaves deverão ser gerados somente pelo titular do certificado correspondente. Os procedimentos específicos devem ser descritos em cada PC implementada.

6.1.1.3. Cada PC implementada pela AC responsável deve definir 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].

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

Item não aplicável. A DPC deve observar que a geração e a guarda de uma chave privada será de responsabilidade exclusiva do titular do certificado correspondente.

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

6.1.3.1. Neste item, a DPC deve descrever os procedimentos utilizados pela AC responsável para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado.

6.1.3.2. A DPC deve também descrever os procedimentos utilizados para a entrega da chave pública de um solicitante de certificado à AC responsável. Os procedimentos específicos aplicáveis devem ser detalhados em cada PC implementada.

### 6.1.4. Disponibilização de chave pública da AC para usuários

Neste item, a DPC deve definir as formas para a disponibilização do certificado da AC responsável, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, as quais poderão compreender, entre outras:

a) No momento da disponibilização de um certificado para seu titular; usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].
b) Diretório;
c) Página *web* da AC; e
d) Outros meios seguros aprovados pelo CG da ICP-Brasil.

### 6.1.5. Tamanhos de chave

6.1.5.1. Neste item, a DPC deve observar que cada PC implementada pela AC responsável definirá o tamanho 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. Caso a AC responsável emita certificados para outras ACs, neste item deve ser também informado o tamanho das chaves criptográficas associadas a esses certificados, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 6.1.6. Geração de parâmetros de chaves assimétricas

A DPC deve prever que os parâmetros de geração de chaves assimétricas da AC responsável adotarão o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 6.1.8. Geração de chave por hardware *ou* software

6.1.8.1. Neste item, a DPC deve indicar se o processo de geração do par de chaves da AC responsável é feito por hardware ou por software. A geração por software será admitida apenas para chaves de AC utilizadas exclusivamente para assinatura de certificados dos tipos A1 ou S1.

6.1.8.2. Cada PC implementada pela AC responsável deve caracterizar 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].

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

6.1.9.1. Neste item, a DPC deve especificar os propósitos para os quais poderão ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC responsável, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados

correspondentes. Cada PC implementada deve especificar os propósitos específicos aplicáveis.

6.1.9.2. A chave privada da AC responsável deverá ser utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

### 6.2. Proteção da Chave Privada

Nos itens seguintes, a DPC deve definir os requisitos para a proteção das chaves privadas da AC responsável. Chaves privadas deverão trafegar cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento. Quando aplicável, a DPC deve também definir os requisitos para a proteção das chaves privadas das ARs vinculadas e das entidades titulares de certificados emitidos pela AC. Cada PC implementada deve especificar os requisitos específicos aplicáveis.

#### 6.2.1. Padrões para módulo criptográfico

6.2.1.1. A DPC deve prever que o módulo criptográfico de geração de chaves assimétricas da AC responsável adotará o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. A DPC deve também, quando cabível, especificar os padrões - como, por exemplo, aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] - requeridos para os módulos de geração de chaves criptográficas dos titulares de certificado. Cada PC implementada deve especificar os requisitos adicionais aplicáveis.

#### 6.2.2. Controle “n de m” para chave privada

6.2.2.1. Neste item, quando cabível, deve ser definida a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”, requerido para a utilização das chaves privadas.

6.2.2.2. A DPC deve estabelecer a exigência de controle múltiplo para a utilização da chave privada da AC responsável. Pelo menos 2 (dois) detentores de partição de chave, formalmente designados pela AC, deverão ser requeridos para a utilização de sua chave privada.

#### 6.2.3. Recuperação (*escrow*) de chave privada

Neste item, a DPC deve observar que não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

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

6.2.4.1. A DPC deve observar que, 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 responsável pela DPC deverá manter cópia de segurança de sua própria chave privada.

6.2.4.3. A AC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido. Cada PC deve definir os requisitos específicos aplicáveis.

6.2.4.4. Em qualquer caso, a cópia de segurança deverá 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. Neste item da DPC, devem ser definidos, quando cabíveis, os requisitos para arquivamento de chaves privadas de sigilo. As chaves deverão ser arquivadas com um nível de segurança não inferior àquele definido para a chave original. Não devem ser arquivadas chaves privadas de assinatura digital.

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

Neste item da DPC, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada da AC responsável em módulo criptográfico. A RFC 2510 poderá ser utilizada para esse fim. Cada PC implementada deve definir, quando aplicáveis, os requisitos para inserção da chave privada dos titulares de certificado em módulo criptográfico.

### 6.2.7. Método de ativação de chave privada

Neste item da DPC devem ser descritos os requisitos e os procedimentos necessários para a ativação da chave privada da AC responsável. Devem ser definidos os agentes autorizados a ativar essa chave, o método de confirmação da identidade desses agentes (senhas, *tokens* ou biometria) e as ações necessárias para a ativação. Cada PC implementada deve descrever os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

### 6.2.8. Método de desativação de chave privada

Neste item da DPC devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada da AC responsável. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias. Cada PC implementada deve descrever os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

### 6.2.9. Método de destruição de chave privada

Neste item da DPC devem ser descritos os requisitos e os procedimentos necessários para destruição da chave privada da AC responsável e de suas cópias de segurança. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias, tais como destruição física, sobrescrita ou apagamento das mídias de armazenamento. Cada PC implementada deve descrever os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

## 6.3. Outros Aspectos do Gerenciamento do Par de Chaves

### 6.3.1. Arquivamento de chave pública

A DPC deve prever que as chaves públicas da AC responsável e dos titulares de certificados de assinatura digital, bem como as LCRs emitidas serão armazenadas pela AC emissora, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

### 6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas da AC responsável pela DPC e dos titulares de certificados de assinatura digital por ela emitidos deverão ser utilizadas apenas durante o período de validade dos certificados

correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Os períodos de uso das chaves correspondentes aos certificados de sigilo emitidos pela AC responsável pela DPC devem ser definidos nas respectivas PCs.

6.3.2.3. Cada PC implementada pela AC responsável deve definir o período máximo de validade do certificado que define, 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 certificados de AC é de 8 (oito) anos.

### 6.4. Dados de Ativação

Nos itens seguintes da DPC, devem ser 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. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

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

6.4.1.1. A DPC deve garantir que os dados de ativação da chave privada da AC responsável serão únicos e aleatórios.

6.4.1.2. Cada PC implementada deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão únicos e aleatórios.

#### 6.4.2. Proteção dos dados de ativação

6.4.2.1. A DPC deve garantir que os dados de ativação da chave privada da AC responsável serão protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

6.4.2.2. Cada PC implementada deve garantir que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, serão protegidos contra uso não autorizado.

### 6.4.3. Outros aspectos dos dados de ativação

Neste item da DPC, quando for o caso, devem ser definidos outros aspectos referentes aos dados de ativação. Entre esses outros aspectos podem ser considerados alguns daqueles tratados, em relação às chaves, nos itens de 6.1 a 6.3.

## 6.5. Controles de Segurança Computacional

### 6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A DPC deve prever que a geração do par de chaves da AC responsável será realizada *off-line*, para impedir o acesso remoto não autorizado.

6.5.1.2. Neste item, a DPC deve também descrever os requisitos gerais de segurança computacional do equipamento onde serão gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC responsável. Os requisitos específicos aplicáveis devem ser descritos em cada PC implementada.

6.5.1.3 Cada computador servidor da AC responsável, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, deverá implementar, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
d) Geração e armazenamento de registros de auditoria da AC;
e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) Mecanismos para cópias de segurança (*backup*).

6.5.1.4. Essas características deverão ser 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 deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão

ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC. Todos esses eventos deverão ser registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC deverá ser preparado e configurado como previsto na PS 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

Neste item da DPC deve ser informada, quando disponível, a classificação atribuída à segurança computacional da AC responsável, segundo critérios como: *Trusted System Evaluation Criteria* (TCSEC), *Canadian Trusted Products Evaluation Criteria*, *European Information Technology Security Evaluation Criteria* (ITSEC) ou o *Common Criteria*.

### 6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Neste item, a DPC deve descrever 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.

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

## 6.6. Controles Técnicos do Ciclo de Vida

Nos itens seguintes da DPC devem ser descritos, quando aplicáveis, os controles implementados pela AC responsável e pelas ARs a ela vinculadas no desenvolvimento de sistemas e no gerenciamento de segurança.

### 6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. Neste item da DPC devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao software do sistema de certificação da AC ou a qualquer outro software desenvolvido ou utilizado pela AC responsável.

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

### 6.6.2. Controles de gerenciamento de segurança

6.6.2.1. Neste item da DPC devem ser descritas as ferramentas e os procedimentos empregados pela AC responsável e pelas ARs vinculadas para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.6.2.2. Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação e a contínua manutenção do sistema de certificação da AC.

### 6.6.3. Classificações de segurança de ciclo de vida

Neste item da DPC deve ser informado, quando disponível, o nível de maturidade atribuído ao ciclo de vida de cada sistema, com base em critérios como: *Trusted Software Development Methodology* (TSDM) ou o *Capability Maturity Model* do *Software Engineering Institute* (CMM-SEI).

### 6.6.4. Controles na Geração de LCR

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

## 6.7. Controles de Segurança de Rede

### 6.7.1. Diretrizes Gerais

6.7.1.1. Neste item da DPC devem ser descritos os controles relativos à segurança da rede da AC responsável, incluindo *firewalls* e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC, somente os serviços estritamente necessários para o funcionamento da aplicação deverão ser habilitados.

6.7.1.3. Todos 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, deverão estar localizados e operar em ambiente de nível, no mínimo, 4.

6.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes deverão ser

implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar 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* deverão ser implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um *firewall* deverá promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC.

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

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

6.7.3.1. O sistema de detecção de intrusão deverá ter capacidade de ser configurado para reconhecer ataques em tempo real e responde-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 sistema de detecção de intrusão deverá ter 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 sistema de detecção de intrusão deverá prover o registro dos eventos em *logs*, 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 – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A freqüência de exame dos arquivos de registro deverá ser, no mínimo, diária e todas as ações tomadas em decorrência desse

exame deverão ser documentadas.

### 6.8. Controles de Engenharia do Módulo Criptográfico

Este item da DPC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC responsável. Poderão ser indicados padrões de referência, como aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]

## 7. PERFIS DE CERTIFICADO E LCR

### 7.1. Diretrizes Gerais

7.1.1. Nos seguintes itens da DPC devem ser descritos os aspectos dos certificados e LCR emitidos pela AC responsável.

7.1.2. Cada PC implementada pela AC responsável deve especificar os formatos dos certificados gerados e das correspondentes LCRs. Devem ser incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

7.1.3. Caso a AC responsável emita certificados para outras ACs, nos itens seguintes deve também ser especificado o formato desses certificados.

### 7.2. Perfil do Certificado

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

#### 7.2.1. Número(s) de versão

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

#### 7.2.2. Extensões de certificado

A ICP-Brasil define como obrigatórias as seguintes extensões para certificados de AC:

a) “***Authority Key Identifier*”, não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública da AC que emite o certificado;

b) "***Subject Key Identifier*", não crítica**: deve conter o *hash* SHA-1 da chave pública da AC titular do certificado;
c) "***Key Usage*", crítica**: somente os bits keyCertSign e cRLSign devem estar ativados;
d) "***Certificate Policies*", não crítica**:
   d.1) o campo policyIdentifier deve conter:
      i. o OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs; ou
      ii. os OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;
   d.2) o campo **policyQualifiers** deve conter o endereço *Web* da DPC da AC que emite o certificado;
e) "***Basic Constraints*", crítica**: deve conter o campo cA=*True*; e
f) "***CRL Distribution Points***", **não crítica**: deve conter o endereço na *Web* onde se obtém a LCR correspondente ao certificado.

### 7.2.3. Identificadores de algoritmo

Os certificados de AC deverão ser assinados com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

### 7.2.4. Formatos de nome

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

**C** = BR

**O** = ICP-Brasil

**OU** = nome da AC emitente

**CN** = nome da AC titular

### 7.2.5. Restrições de nome

Neste item da DPC, devem ser descritas as restrições aplicáveis para os nomes de AC titulares de certificados, em conformidade com as restrições gerais estabelecidas pela ICP-Brasil no documento

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

### 7.2.6. OID (*Object Identifier*) de DPC

Neste item, deve ser informado o OID da DPC.

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

A extensão "*Policy Constraints*" poderá ser utilizada, da forma definida na RFC 5280, em certificados emitidos pela AC responsável para outras ACs.

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

Em certificados de AC, o campo policyQualifiers da extensão "*Certificate Policies*" deverá conter o endereço *web* (URL) da DPC da AC que emite o certificado.

### 7.2.9. Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

## 7.3. Perfil de LCR

### 7.3.1. Número(s) de versão

As LCRs geradas pela AC responsável deverão implementar a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

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

7.3.2.1. Neste item, a DPC deve descrever todas as extensões de LCR utilizadas pela AC responsável e sua criticalidade.

7.3.2.2. 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 seqüencial para cada LCR emitida pela AC.

## 8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes devem definir como será mantida e administrada a DPC.

### 8.1. Procedimentos de mudança de especificação

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na DPC. Qualquer alteração na DPC deverá ser submetida à aprovação da AC Raiz.
A DPC deverá ser atualizada sempre que uma nova PC implementada pela AC responsável o exigir.

### 8.2. Políticas de publicação e notificação

Neste item devem ser descritos os mecanismos empregados para a distribuição da DPC à comunidade envolvida.

### 8.3. Procedimentos de aprovação

Toda DPC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

## 9. DOCUMENTOS REFERENCIADOS

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

| *Ref.* | *Nome do documento* | *Código* |
|---|---|---|
| **[2]** | CRITÉRIOS E PROCEDIMENTOS PARA 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** |
| **[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** |

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

| *Ref.* | *Nome do documento* | *Código* |
|---|---|---|
| **[1]** | CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL | **DOC-ICP-03.01** |
| **[9]** | PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL | **DOC-ICP-01.01** |

9.3. Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio http://www.iti.gov.br .

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