ALTERADA EM 26.04.2002 PELA RESOLUÇÃO 13.
ALTERADA EM 29.08.2003 PELA RESOLUÇÃO 21.
ALTERADA EM 24.12.2003 PELA RESOLUÇÃO 26.
ALTERADA EM 29.01.2004 PELA RESOLUÇÃO 31.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 34.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 37.
ITENS 1.3.2.1 E 1.3.2.2. REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42.
REVOGADOS EM 18.04.2006 PELA RESOLUÇÃO 40.

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 8, DE 12 DE DEZEMBRO DE 2001.

Aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil.

O **SECRETÁRIO-EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL** faz saber que aquele Comitê, no uso das atribuições previstas nos incisos I, III, V e VI do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Art. 1º Ficam aprovados os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL conforme estabelecidos em anexo.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

MURILO MARQUES BARBOZA

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

1. INTRODUÇÃO

1.1. Visão Geral

Este documento estabelece requisitos mínimos de observância obrigatória pelas Autoridades Certificadoras (AC) integrantes da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Declarações de Práticas de Certificação (DPC). A Declaração de Práticas de Certificação é o documento que descreve as práticas e os procedimentos empregados pela Autoridade Certificadora na execução de seus serviços.

Toda Declaração de Práticas de Certificação elaborada no âmbito da ICP-Brasil deve obrigatoriamente adotar a mesma estrutura empregada neste documento.

1.2. Identificação

Neste item deve ser identificada a Declaração de Práticas de Certificação 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 a 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 à Declaração de Práticas de Certificação.

1.3.2. Autoridades de Registro (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser identificadas as Autoridades de Registro (AR) 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 DPC deverá ser atualizada sempre que houver o credenciamento de mais uma AR vinculada à AC responsável.

1.3.2.1. Novos endereços de instalações técnicas (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

A Autoridade de Registro já credenciada na ICP-Brasil poderá abrir novos endereços de instalações técnicas desde que encaminhe, por intermédio da cadeia de Autoridades Certificadoras operacionalmente vinculadas, solicitação de funcionamento à Autoridade Certificadora Raiz, acompanhada dos seguintes documentos:

a) formulário constante dos itens 1 e 2 do Anexo II-A da Resolução Nº 6, de 22 de novembro de 2001 indicando os novos endereços;

b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais; e

c) relação das pessoas responsáveis por cada um dos novos postos da AR.

Estando a documentação regular, a AC Raiz autorizará o funcionamento dos novos postos mediante intimação da solicitante, que a partir deste momento disponibilizará os novos endereços em seu sítio.

A AC Raiz poderá, a qualquer tempo, verificar a conformidade dos procedimentos e atividades dos postos das Autoridades de Registro autorizados com as práticas e regras estabelecidas pelo CG da ICP-Brasil. Constatada qualquer irregularidade em uma das instalações técnicas, a AC Raiz cassará imediatamente a autorização de funcionamento deste posto e verificará a conformidade dos procedimentos de qualquer outro posto da mesma AR. Verificando-se mais uma vez

irregularidades, todos os postos que adotarem os mesmos procedimentos também terão sua autorização cassada.

1.3.2.2. Posto provisório de instalação técnica (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

A Autoridade de Registro já credenciada na ICP-Brasil poderá, ainda, abrir postos provisórios de instalações técnicas desde que encaminhe, por intermédio da cadeia de Autoridades Certificadoras operacionalmente vinculadas, solicitação de funcionamento à Autoridade Certificadora Raiz, com no mínimo 10 (dez) dias de antecedência, acompanhada dos seguintes documentos:

a) formulário contante do Anexo II-B da Resolução n. 6, de 22 de novembro de 2001;

b) indicação dos procedimentos que serão adotados quanto aos aspectos de segurança e operacionais;

c) indicação da pessoa responsável pelo posto provisório; e

d) relação dos agentes de registro que trabalharão no posto provisório.

Estando a documentação regular, a AC Raiz autorizará o funcionamento do posto provisório mediante intimação da solicitante.

1.3.3. Titulares de Certificado (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003).

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 AC para as quais a AC em questão poderá emitir certificados.

NOTA 1: 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.

NOTA 2: 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.

1.3.4. Aplicabilidade

Este item da DPC deve relacionar e identificar as Políticas de Certificado (PC) implementadas pela AC responsável, que definem como os certificados emitidos deverão ser utilizados pela comunidade. Nas PC estarão relacionadas às 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. Os requisitos específicos associados a essas obrigações devem estar detalhados nas PC implementadas pela AC responsável pela DPC.

2.1.1 Obrigações da AC (REDAÇÃO DADA PELA RESOLUÇÃO Nº 37, DE 21 DE OUTUBRO DE 2004).

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

- operar de acordo com a sua DPC e com as PC que implementa;
-
- gerar e gerenciar o seu par de chaves criptográficas;
-
- assegurar a proteção de suas chaves privadas;
-
- notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
-
- notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades;
-
- distribuir o seu próprio certificado;
-
- emitir, expedir e distribuir os certificados de AC de nível imediatamente subseqüente ao seu ou os certificados de AR vinculadas e de usuários finais;
-
- informar a emissão do certificado ao respectivo solicitante;

- revogar os certificados por ela emitidos;

- emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *On-line Certificate Status Protocol*);

- publicar em sua página *Web* sua DPC e as PC aprovadas que implementa;

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

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

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

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

- manter e testar regularmente seu Plano de Continuidade do Negócio;

- 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 AC de nível subseqüente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil;

- 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; e

- não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2. Obrigações das AR (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003).

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

- receber solicitações de emissão ou de revogação de certificados;

- confirmar a identidade do solicitante e a validade da solicitação;

- encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável utilizando VPN (V*irtual Private Network* - rede privativa virtual), SSL (S*ecure Socket Layer* - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;

- utilizar VPN (*Virtual Private Network* - rede privativa virtual), SSL (*Secure Socket Layer* - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

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

- disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;

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

- manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada;

- manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil; e

- oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3. Obrigações do Titular do Certificado (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos pela AC responsável pela DPC, que integrarão o contrato de que trata o item 4.1, contendo, no mínimo, as abaixo relacionadas:

- fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
-
- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
-
- utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
-
- conhecer os seus direitos e obrigações, contemplados pela DPC, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; 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*)

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

Constituem direitos da terceira parte:

- recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;

- verificar a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
-
- não constar da LCR da AC emitente;
-

- não estiver expirado; e
-
- puder ser verificado com o uso de certificado válido da AC emitente;

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:

- disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e a sua LCR;
-
- estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
-
- implementar os recursos necessários para a segurança dos dados nele armazenados.

2.2. Responsabilidades

2.2.1. Responsabilidades da AC (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

A AC responde pelos danos a que der causa.

A AC responsável pela DPC responderá solidariamente pelos atos das AC das cadeias a ela subordinadas.

2.2.2. Responsabilidades da AR (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

A AR será responsável pelos danos a que der causa.

A AC responsável pela DPC responderá solidariamente pelos atos das AR a ela vinculadas.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (*Relying Party*)
Neste item devem ser estabelecido a inexistência de responsabilidade da terceira parte (*Relying Party*) perante a AC ou AR a elas vinculadas, exceto na hipótese de prática de ato ilícito.

2.3.2. Relações Fiduciárias (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Neste item deve constar que a AC responsável ou AR vinculada indenizará integralmente os danos o 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 AR 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

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.

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. Procedimentos de solução de disputa

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.

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

2.5. Tarifas de Serviço

Nos itens a seguir, devem ser especificadas pela AC responsável pela DPC as políticas tarifária e de reembolso aplicáveis para cada PC implementada.

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 a 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 (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

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% (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

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

- seu próprio certificado;
- suas LCR;
- sua DPC;
- as PC que implementa; e
- os endereços das instalações técnicas das AR vinculadas.

2.6.2. Freqüência de publicação

Neste item deve ser informada a freqüência de publicação das informações de que trata o item anterior.

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:

- localização lógica;

- disponibilidade;
-
- protocolos de acesso; e
-
- requisitos de segurança.

2.7. Auditoria de Conformidade

A AC Raiz é a responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR a elas vinculadas. A auditoria dessas entidades é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, Política de Segurança e demais normas e procedimentos estabelecidos pela ICP-Brasil.

A AC responsável pela DPC deverá disponibilizar à AC Raiz e às AC de nível imediatamente superior relatórios anuais de auditoria das entidades da ICP-Brasil a ela vinculadas diretamente.

Considera-se prestador de serviço de suporte aquele que desempenha atividade descrita neste documento ou em uma PC implementada pela AC responsável.

Os itens seguintes da DPC devem detalhar aspectos relacionados a esse processo de auditoria.

2.7.1. Freqüência de auditoria de conformidade

Neste item da DPC, deve ser informada a freqüência da auditoria das entidades diretamente vinculadas à AC responsável. Essa freqüência deverá ser, no mínimo, anual.

2.7.2. Identidade e qualificações do auditor (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Os relatórios de auditoria das AC de nível imediatamente subseqüente (AC Subseqüente) à AC responsável (AC Principal) deverão ser fornecidos por empresa de auditoria especializada e independente, contratada pela AC a ser auditada e autorizada pela AC Raiz.

Os relatórios de auditoria das AR e dos prestadores de serviço de suporte não precisam ser fornecidos por empresa de auditoria especializada e independente.

2.7.3. Relação entre auditor e parte auditada

2.7.4. Tópicos cobertos pela auditoria

2.7.5. Medidas adotadas em caso de não conformidade

2.7.6. Comunicação de resultados

Os relatórios completos das auditorias deverão ser entregues à AC Raiz.

2.8. Sigilo (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

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.

A DPC deve informar que os titulares de certificados 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.

No caso de certificados de sigilo emitidos pela AC, a DPC deve se referir às PC correspondentes para delimitar as responsabilidades pela manutenção e pela garantia do sigilo das respectivas chaves privadas.

2.8.1. Tipos de informações sigilosas

Neste item devem ser identificados os tipos de informações consideradas sigilosas pela AC responsável

pela DPC e pelas AR a ela vinculadas, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

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

2.8.2. Tipos de informações não sigilosas

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

- os certificados e as LCR emitidos pela AC;
-
- informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
-
- as PC implementadas pela AC;
-
- a DPC da AC;
- versões públicas de Políticas de Segurança; e
-
- resultados finais de auditorias.
-

2.8.3. Divulgação de informação de revogação ou suspensão de certificado. (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

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.

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

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

2.8.4. 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.

2.8.5. Informações a terceiros

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

2.8.6. Divulgação por solicitação do titular

Neste item devem ser descritas as condições sob as quais um titular de certificado emitido pela AC, 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.

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

2.8.7. 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 (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item e nos seguintes, a DPC deve descrever os requisitos e os procedimentos gerais utilizados pelas AR vinculadas à AC responsável no processo inicial de identificação dos solicitantes de certificado. Os requisitos e procedimentos específicos devem estar detalhados nas PC implementadas pela AC responsável pela DPC.
A AR realizará a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de no mínimo dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1. Tipos de nomes

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).

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

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

3.1.5. 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.

3.1.6. 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.

3.1.7. Método para comprovar a posse de chave privada

A DPC deve indicar os procedimentos executados pela AC responsável ou pelas AR 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*). Os métodos devem estar detalhados nas PC implementadas pela AC responsável pela DPC.

3.1.8. Autenticação da identidade de uma organização (REDAÇÃO DADA PELA RESOLUÇÃO Nº 31, DE 29 DE JANEIRO DE 2004)

Neste item devem ser descritos, se for o caso, os procedimentos adotados pela AC responsável pela DPC para a identificação de uma AC de nível imediatamente subseqüente ao seu. Esta identificação poderá estar restrita aos procedimentos descritos no documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.

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

- registro comercial, no caso de empresa individual;
- ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e , no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ); e
- prova de inscrição no Cadastro Específico do INSS (CEI), se aplicável.

A pessoa física responsável referida no item 3.1.1 também deverá ser identificada, na forma descrita no item seguinte.

3.1.9. Autenticação da identidade de um indivíduo (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

Neste item da DPC devem ser descritos os procedimentos gerais empregados pelas AR 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.

Cada PC implementada pela AC responsável deve definir os documentos de identificação exigidos, com base nos requisitos aplicáveis estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil.

A DPC deve estabelecer que solicitações de certificados para AC deverão ser realizadas por pessoa física legalmente responsável. Caberá às AR vinculadas à AC responsável verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos. Os procedimentos utilizados pelas AR para identificação e verificação da autorização do solicitante devem ser descritos em detalhes nas PC implementadas.

A DPC deve estabelecer, ainda, que no caso de certificado emitido para pessoa física, o titular deste assinará “termo de titularidade”, a ser mantido junto à documentação exigida neste item, e será, para todos os efeitos legais responsável pela correta utilização do certificado conforme as normas da ICP-Brasil, assim como pelos danos a que der causa pelo uso indevido do certificado.

No caso de certificado emitido para pessoa jurídica, o seu representante legal assinará “termo de titularidade”, e a pessoa física indicada como responsável pelo certificado assinará “termo de responsabilidade”. Os termos de titularidade e de responsabilidade serão mantidos junto à documentação exigida neste item. Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

No caso de certificado emitido para equipamento ou aplicação, também serão assinados “termo de titularidade” e “termo de responsabilidade”, sendo o titular do certificado e a pessoa física designada, responsáveis pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

A DPC deve ainda prever que deverá ser mantido arquivo com o tipo e os detalhes do procedimento de identificação utilizado em cada caso.

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

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. Os processos específicos requeridos pelas PC implementadas devem ser descritos nessas PC.

3.3. Geração de novo par de chaves após revogação

Neste item, a DPC deve descrever os procedimentos utilizados para confirmação da identidade de uma entidade solicitante de novo certificado, após a revogação do certificado dessa entidade. Os procedimentos detalhados devem ser descritos nas PC implementadas.

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 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 documentadas. Os procedimentos detalhados devem ser descritos nas PC implementadas.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado (REDAÇÃO DADA PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

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

- a comprovação de atributos de identificação constantes do certificado;
- a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de nível A3; e
- um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, se for o caso, estabelecendo as condições de uso deste.

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 (Critérios e Procedimentos para credenciamento das Entidades integrantes da ICP-Brasil).

Nesse caso, aquela AC deverá encaminhar a solicitação de seu certificado à AC emitente por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10

4.2. Emissão de Certificado

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. Os procedimentos detalhados devem ser descritos nas PC implementadas.

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

4.3. Aceitação de Certificado (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

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. Os procedimentos detalhados devem ser descritos nas PC implementadas.

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.

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

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

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

- quando constatada emissão imprópria ou defeituosa do mesmo;
- quando for necessária a alteração de qualquer informação constante no mesmo;
- no caso de dissolução de AC titular do certificado; ou
- no caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

A DPC deve observar ainda que:

- 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
- 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:

- Por solicitação do titular do certificado;
- Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
- Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- pela AC emitente;
- por uma AR vinculada; ou
- por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3. Procedimento para solicitação de revogação

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. Os procedimentos detalhados devem ser descritos nas PC implementadas.

Como diretrizes gerais, a DPC deve estabelecer que:

- o solicitante da revogação de um certificado será identificado;
- as solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;
- as justificativas para a revogação de um certificado serão documentadas; e
- 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.

Cada PC implementada pela AC responsável, deve definir o prazo limite para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, com base nos requisitos aplicáveis

estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil.

O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 24 (vinte e quatro) horas.

4.4.4. Prazo para solicitação de revogação

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.

Cada PC implementada pela AC responsável 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.

4.4.5. 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

Cada PC implementada pela AC responsável deve definir a freqüência de emissão da LCR associada, com base nos requisitos aplicáveis estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil.

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

O prazo máximo admitido para a emissão de LCR referente a certificados de AC é de 15 (quinze) 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 AC de nível imediatamente subseqüente ao seu.

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

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 poderá 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*). Os detalhes devem ser descritos nas PC implementadas.

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, de informações de revogação de certificados, pelas terceiras partes(*relying parties*).

4.4.15. Requisitos especiais para o caso de comprometimento de chave

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 imediatamente a AC emitente. Os requisitos específicos devem ser descritos nas PC implementadas.

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

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:

- iniciação e desligamento do sistema de certificação;
- tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
- mudanças na configuração da AC ou nas suas chaves;
- mudanças nas políticas de criação de certificados;
- tentativas de acesso (*login*) e de saída do sistema (*logoff*);
- tentativas não-autorizadas de acesso aos arquivos de sistema;
- geração de chaves próprias da AC ou de chaves de seus usuários finais;
- emissão e revogação de certificados;
- geração de LCR;
- tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- operações de escrita nesse repositório, quando aplicável.

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

- registros de acessos físicos;
- manutenção e mudanças na configuração de seus sistemas;

–
– mudanças de pessoal e de perfis qualificados;
–
– relatórios de discrepância e comprometimento; e
–
– registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

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.

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.

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

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.

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

Os mecanismos de proteção descritos neste item devem obedecer à Política de Segurança da ICP-Brasil.

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 AR 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:

- solicitações de certificados;
- solicitações de revogação de certificados;
- notificações de comprometimento de chaves privadas;
- emissões e revogações de certificados;
- emissões de LCR;
- trocas de chaves criptográficas da AC responsável; e
- 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:

- as LCR referentes a certificados de assinatura digital deverão ser retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados; e
- as demais informações 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.

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

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.

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

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 (*time-stamping*) 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 AR vinculadas para a obtenção ou a verificação de suas informações de arquivo.

4.7. Troca de chave

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.

Os procedimentos aplicáveis detalhados devem estar descritos em cada PC implementada, onde pode ser definido prazo anterior à data de expiração do certificado, no qual a AC ou uma AR vinculada comunicará o seu titular para que seja solicitada a emissão de um novo certificado.

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 Plano de Continuidade do Negócio da AC responsável, estabelecido conforme a Política de Segurança da ICP-Brasil, 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.

4.9. Extinção da AC (REDAÇÃO DADA PELA RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003)

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 a ela vinculada. Devem ser descritos os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo.

O responsável pela guarda desses dados e registros deverá observar os mesmos requisitos de segurança exigidos para a AC extinta.

As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC que encerra as suas atividades.

A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

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

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 AR 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 AR vinculadas.

5.1.1. Construção e localização das instalações

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.

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

- 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;
- instalações para sistemas de telecomunicações;
- sistemas de aterramento e de proteção contra descargas atmosféricas; e
- iluminação de emergência.

5.1.2. Acesso físico

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 e os requisitos que seguem.

5.1.2.1. Níveis de acesso

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.

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.

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.

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.

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.

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.

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.

No quarto nível (nível 4), interior ao terceiro, é onde deverão ocorrer atividades especialmente sensíveis da operação da AC tais como emissão e revogação de certificados, e 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.

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.

As salas-cofre deverão ser construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

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

- equipamentos de produção *on-line* e cofre de armazenamento;
- equipamentos de produção *off-line* e cofre de armazenamento; e
- equipamentos de rede e infra-estrutura (*firewall*, roteadores, *switches* e servidores).

O quinto nível (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.

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

- ser feito em aço ou material de resistência equivalente; e
- possuir tranca com chave.

O sexto nível (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

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.

As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 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, uma fita referente a cada semana. Essas fitas deverão ser armazenadas em ambiente de terceiro nível.

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.

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.

O sistema de notificação de alarmes deverá utilizar pelo menos 2 (dois) meios de notificação: sonoro e visual.

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

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.

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

A infra-estrutura 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.

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

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.

Todos os cabos deverão ser catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

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. Qualquer modificação nessa rede deverá ser previamente documentada.
Não deverão ser admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

O sistema de climatização deverá atender os 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 à falhas.

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

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

A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC deverá ser garantida, por meio de:

- geradores de porte compatível;
- geradores de reserva;
- sistemas de *no-breaks* redundantes; e
- sistemas redundantes de ar condicionado.

5.1.4. Exposição à água

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

5.1.5.Prevenção e proteção contra incêndio

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.

Nas instalações da AC não será permitido fumar ou portar objetos que produzam fogo ou faísca.

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.

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

5.1.6. Armazenamento de mídia

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

Todos os documentos em papel que contenham informações classificadas como sensíveis deverão ser triturados antes de ir para o lixo.

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*)

As instalações de *backup* deverão atender os 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.

5.2. 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 AR 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

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.

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.

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.

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

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.

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

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

- ser incluído em uma lista de acesso às instalações da AC;
- ser incluído em uma lista para acesso físico ao sistema de certificação da AC;
- receber um certificado para executar suas atividades operacionais na AC; e
- receber uma conta no sistema de certificação da AC.

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

- ser diretamente atribuídos a um único empregado;
- não ser compartilhados; e
- ser restritos às ações associadas ao perfil para o qual foram criados.

A AC deverá implementar um padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, 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 e pelas AR vinculadas 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 AR vinculadas encarregados de tarefas

operacionais terão registrado em contrato ou termo de responsabilidade:

- os termos e as condições do perfil que ocuparão;
- o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
- 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 AR 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. A AC responsável poderá definir requisitos adicionais para a admissão.

5.3.2. Procedimentos de verificação de antecedentes

Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC responsável e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá ser submetido a:

- verificação de antecedentes criminais;
- verificação de situação de crédito;
- verificação de histórico de empregos anteriores; e
- comprovação de escolaridade e de residência.

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 AR 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:

- princípios e mecanismos de segurança da AC e das AR vinculadas;
- sistema de certificação em uso na AC;
- procedimentos de recuperação de desastres e de continuidade do negócio; 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 AR 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 AR.

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 AR 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

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 suspender o acesso dessa pessoa ao seu sistema de certificação e tomar as medidas administrativas e

legais cabíveis.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC responsável e das AR 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. A AC responsável poderá definir requisitos adicionais para a contratação.

5.3.8. Documentação fornecida ao pessoal

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

- sua DPC;
- as PC que implementa;
- a Política de Segurança da ICP-Brasil;
- documentação operacional relativa a suas atividades; e
- contratos, normas e políticas relevantes para suas atividades.

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 AR vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves (REDAÇÃO DADA PELA RESOLUÇÃO 13, DE 26 DE ABRIL DE 2002)

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.

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.

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 Políticas de Certificado na ICP-Brasil

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

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.

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:

- formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- diretório;
- página *Web* da AC; e
- outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

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 Políticas de Certificado na ICP-Brasil.

Caso a AC responsável emita certificados para outras AC, neste item deve ser também informado o tamanho das chaves criptográficas associadas a esses certificados. O tamanho mínimo admitido pela ICP-Brasil para chaves criptográficas associadas a certificados de AC é de 2048 (dois mil e quarenta e oito) bits.

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 FIPS (*Federal Information Processing Standards*) 140-1, no mínimo *level* 2.

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*).

6.1.8. Geração de chave por *hardware ou software*

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.

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 Políticas de Certificado na ICP-Brasil.

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

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.

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 AR 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

A DPC deve prever que o módulo criptográfico de geração de chaves assimétricas da AC responsável adotará o padrão FIPS (*Federal Information Processing Standards*) 140-1, no mínimo, *level* 2.

A DPC deve também, quando cabível, especificar os padrões - como, por exemplo, o padrão FIPS 140-1 - 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

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.

A DPC deve estabelecer a exigência de controle múltiplo para a utilização da chave privada da AC responsável. Pelo menos 2 (dois) empregados da AC com perfis qualificados 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

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.

A AC responsável pela DPC deverá manter cópia de segurança de sua própria chave privada.

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.

Em qualquer caso, a cópia de segurança deverá ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

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.

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 por ela emitidos deverão permanecer armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade. Cada PC de assinatura digital implementada deve descrever os períodos de arquivamento da chave pública de entidade titular de certificado.

6.3.2. Períodos de uso para as chaves pública e privada (REDAÇÃO DADA PELA RESOLUÇÃO Nº 34 DE 21 DE OUTUBRO DE 2004)

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.

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

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 Políticas de Certificado na ICP-Brasil.

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

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

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

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.

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

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.

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.

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:

- controle de acesso aos serviços e perfis da AC;
- clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
- uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- geração e armazenamento de registros de auditoria da AC;
- mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- mecanismos para cópias de segurança (*backup*).

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.

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.

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

6.5.2. Classificação da segurança computacional

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*.

6.6. Controles Técnicos do Ciclo de Vida

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

6.6.1. Controles de desenvolvimento de sistema

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.

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

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

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).

6.7. Controles de Segurança de Rede

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

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

Todos os servidores e elementos de infra-estrutura 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.

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.

O acesso lógico aos elementos de infra-estrutura 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.

6.7.1. *Firewall*

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.

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

6.7.2. Sistema de detecção de intrusão (IDS)

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*.

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.

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.

6.7.3. 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 o FIPS (*Federal Information Processing Standards*) 140-1.

7. PERFIS DE CERTIFICADO E LCR

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

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

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

7.1. 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.

7.1.1. 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 2459.

7.1.2. Extensões de certificado

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

- **"*Authority Key Identifier*", não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública da AC que emite o certificado;
- **"*Subject Key Identifier*", não crítica**: deve conter o *hash* SHA-1 da chave pública da AC titular do certificado;
- **"*Key Usage*", crítica**: somente os bits keyCertSign e cRLSign devem estar ativados;
- "***Certificate Policies*", não crítica**: o campo policyIdentifier deve conter:

- o OID da DPC da AC titular do certificado, se essa AC emite certificados para outras AC, e
-
- os OID das PC que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;

–

O campo **policyQualifiers** deve conter o endereço *Web* da DPC da AC que emite o certificado;

- **"*Basic Constraints*", crítica**: deve conter o campo cA=*True*; e

- **"*CRL Distribution Points*"**, **não crítica**: deve conter o endereço na *Web* onde se obtém a LCR correspondente ao certificado.

7.1.3. Identificadores de algoritmo

Os certificados de AC deverão ser assinados com o uso do algoritmo RSA com SHA-1 como função *hash* (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4. 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, da seguinte forma:

C = BR
O = ICP-Brasil
CN = nome da AC

7.1.5. 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 Políticas de Certificado na ICP-Brasil.

7.1.6. OID (*Object Identifier*) de DPC

Neste item, deve ser informado o OID da DPC.

7.1.7. Uso da extensão "*Policy Constraints"*

A extensão "*Policy Constraints"* poderá ser utilizada, da forma definida na RFC 2459, em certificados emitidos pela AC responsável para outras AC.

7.1.8. 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.

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 2459.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC responsável deverão implementar a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2. Extensões de LCR e de suas entradas

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

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

- **"*Authority Key Identifier*"**: deve conter o *hash* SHA-1 da chave pública da AC que assina a LCR; e
- **"*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 Declaração de Práticas de Certificação.

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 do CG da ICP-Brasil.

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 (REDAÇÃO DADA PELA RESOLUÇÃO Nº 13, DE 26 DE AGOSTO DE 2002)

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

ALTERADA EM 26.04.2002 PELA RESOLUÇÃO 13.
ALTERADA EM 29.08.2003 PELA RESOLUÇÃO 21.
ALTERADA EM 24.12.2003 PELA RESOLUÇÃO 26.
ALTERADA EM 29.01.2004 PELA RESOLUÇÃO 31.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 34.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 37.
ITENS 1.3.2.1 E 1.3.2.2. REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42.
REVOGADOS EM 18.04.2006 PELA RESOLUÇÃO 40.