RESOLUÇÃO CG ICP-BRASIL Nº 177, DE 20 DE OUTUBRO DE 2020

Aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil – DOC-ICP-05.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6°, §1°, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4° da Medida Provisória n° 2.200-2, de 24 de agosto de 2001, em plenária por videoconferência realizada em 20 de outubro de 2020,

CONSIDERANDO a determinação estabelecida pelo Decreto n° 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

CONSIDERANDO a necessidade de regulamentar a emissão de certificado digital de pessoa física de forma conjunta com Carteira de Identidade (RG) e Carteira Nacional de Habilitação (CNH),

CONSIDERANDO a necessidade de regulamentar a emissão de certificado digital de pessoa jurídica pelas juntas comerciais, e

CONSIDERANDO que a Lei n° 14.063, de 23 de setembro de 2020, reestabelece o amparo legal para a emissão primária de certificados digitais ICP-Brasil de forma não presencial,

RESOLVEU:

Art. 1° Esta Resolução aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.

Art. 2° Fica aprovada a versão 6.0 do documento DOC-ICP-05 – Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil, anexa a esta Resolução.

Art. 3° Ficam revogadas:

I - a Resolução n° 167, de 17 de abril de 2020;

II - a Resolução n° 164, de 17 de abril de 2020;

III - a Resolução n° 156, de 07 de fevereiro de 2020;

IV - a Resolução n° 153, de 17 de setembro de 2019;

V - a Resolução n° 121, de 06 de julho de 2017;

VI- a Resolução n° 118, de 09 de dezembro de 2015;

VII - a Resolução n° 113, de 30 de setembro de 2015;

VIII - a Resolução n° 107, de 25 de agosto de 2015;

IX - a Resolução n° 84, de 17 de novembro de 2010;

X - a Resolução n° 79, de 28 de maio de 2010;

XI – a Resolução n° 75, de 31 de março de 2010;

XII – a Resolução n° 66, de 09 de junho de 2009;

XIII – a Resolução n° 54, de 28 de novembro de 2008;

XIV – a Resolução n° 48, de 03 de dezembro de 2007; e

XV – a Resolução n° 42, de 18 de abril de 2006

Art. 4° Esta Resolução entra em vigor em 03 de novembro de 2020.

THIAGO MEIRELLES FERNANDES PEREIRA

Infraestrutura de Chaves Públicas Brasileira

ANEXO

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

DOC-ICP-05

Versão 6.1

(Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

22 de janeiro de 2021

(Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução CG ICP-Brasil nº 181, de 22.01.2021 **Versão 6.1**	3.2.3.1 e 3.2.3.1.8	Inclui a previsão de batimento biométrico e biográfico, realizado em base oficial nacional, no processo de identificação de requerente de certificado digital ICP-Brasil.
Resolução nº 177, de 20.10.2020 **Versão 6.0**		Revisão e consolidação do DOC-ICP-05, conforme Decreto nº 10.139, de 28 de novembro de 2019. Regulamenta a emissão de certificado digital de pessoa física de forma conjunta com Carteira de Identidade (RG) e Carteira Nacional de Habilitação (CNH) e a emissão de certificado digital de pessoa jurídica pelas juntas comerciais. Ajustes para emissão por meio de videoconferência.
Resolução 164 e Resolução 167, de 17.04.2020 **Versão 5.5**	5.1.2.2.2, 4.9.3.3, 4.9.3.4 e 4.9.7.3.	Altera o tempo de armazenamento do vídeo resultante da gravação 24x7 e altera os prazos máximos previstos para a emissão de LCR e para a conclusão do processo de revogação de certificado.
Resolução 156, de 07.02.2020 **Versão 5.4**	3.2.3.1.6, 3.2.9.4, 3.2.9.4.1.c e 3.2.9.6	Alteração nos procedimentos para emissão de certificados digitais pelos conselhos de classes profissionais instituídos por lei.
Resolução 155, de 03.12.2019 **Versão 5.3**	3.2, 3.3, 4.1, 4.5.1.2 e 6.2.3	Alteração no procedimento de identificação. Emissão de um novo certificado utilizando procedimento de confirmação de cadastro já

Ato que aprovou a alteração	Item alterado	Descrição da alteração
		realizado.
Resolução 154, de 01.10.2019 **Versão 5.2**	3.2.3.1.3, alínea “b”, 6.1.1.4	Estender a etapa de verificação para AR de PSS da AC. Correção na redação do item 6.1.1.4.
Resolução 153, de 17.09.2019 **Versão 5.1**	3.2.9.3.3 (novo)	Atualização dos procedimentos para emissão de certificados para servidores públicos federais.
Resolução 151, de 30.05.2019 **Versão 5.0**	1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11	Atualização dos requisitos Webtrust e consolidação com a versão 4.7, com a simplificação dos processos da ICP-Brasil.
Resolução 139, de 03.07.2018 **Versão 4.6**	3.1.1.4.1, 3.1.1.11, 3.1.13, 4.4.2	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
Resolução 136, de 08.03.2018 **Versão 4.5**	3.1.10.1.3, 4.1.1.c	Aprovação dos procedimentos para criação do termo de titularidade.
Resolução 131, de 10.11.2017 **Versão 4.4**	3.1.1.10 e 3.1.9	Validação de solicitação de certificados para pessoas físicas titulares de contas de depósito.
Resolução 130, de 19.09.2017 **Versão 4.3**	3.1.1.2	Procedimentos de validação fora do ambiente físico da AR.
Resolução 119 e 121, de 06.07.2017 **Versão 4.2**	2.7.1 e 4.4.10 3.1.9.1, 4.1.1.alínea b, 4.1.1.alínea c, 4.4.2, 2.2.1.4	Obrigatoriedade de realização de auditorias WebTrust e de implementação de respostas OCSP para certificados do tipo SSL/TLS. Procedimentos para emissão de

Ato que aprovou a alteração	Item alterado	Descrição da alteração
		certificados digitais para servidores públicos da ativa e militares da União.
Resolução 118, de 09.12.2015 **Versão 4.1**	2.6.4 e 2.6.4.1	Define a obrigatoriedade da disponibilização de dois repositórios para a distribuição da LCR.
Resolução 115, de 11.11.2015 **Versão 4.0**	3.1.1.8, 3.1.11.1.4, 3.1.11.3.1 e 4.4.2.	Criação de Política de Certificado A CF-e-SAT.
Resolução 114, de 30.09.2015 **Versão 3.9**	3.1.1.1, 3.1.1.7 (novo), 3.1.9, 3.1.9.1	Obrigatoriedade da coleta de dados biométricos do requerente do certificado digital.
Resolução 107, de 25.08.2015 **Versão 3.8**	3.1.1.1, alínea a, item i 3.2.2, alínea b	Limita o prazo de validade para até 90 dias nas procurações. Restringe a renovação automática não presencial apenas para pessoa física.
Resolução 99, de 09.10.2013 **Versão 3.7**	6.3.2.4	Amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolução 90, de 13.08.2012 **Versão 3.6**	3.1.9.1, 6.3.2.4	Inclui as Notas nº 5, 6 e 7 e altera a validade de certificados de AC.
Resolução 84, de 18.11.2010 **Versão 3.5**	2.2.1.3, 3.1.1.6, 3.1.9.1, 3.1.9.2.1, 4.1.1, 4.4.2	Inclui procedimentos para a emissão de certificados digitais que integram o documento de Registro de Identidade Civil-RIC.

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 79, de 07.06.2010 **Versão 3.4**	3.1.1.1	Complementa os requisitos para procuração de pessoa jurídica, para aceitação apenas quando o ato constitutivo prevê.
Resolução 75, de 31.03.2010 **Versão 3.3**	4.6.2, 4.4.11	Altera prazo de retenção do dossiê.
Resolução 74, de 24.11.2009 **Versão 3.2**	2.1.3, 3.1.10.1.3, 3.1.10.3.2 4.1.1, 4.5.1.7, 9.3	Alterações relacionadas aos procedimentos operacionais para utilização de Termo de Titularidade.
Resolução 66, de 06.06.2009 **Versão 3.1**	3.2.2	Altera procedimentos para a renovação de certificados digitais de Pessoa Jurídica.
Resolução 54, de 19.11.2008 **Versão 3.0**	3.1.11.2.2, 4.1.3	Inclusão de referências a Carimbo de Tempo.
Resolução 48, de 03.12.2007 **Versão 2.1**	3.1.10.2 3.1.1.5 6.6.4 3.1.10.2	Alterados os documentos a serem apresentados para identificação de uma organização que solicita certificado digital. Incluído item sobre identificação de Servidores do Serviço Exterior Brasileiro em missão permanente no exterior. Incluído item exigindo verificação de consistência do conteúdo das LCRs, antes de sua publicação. Alterados os documentos a serem apresentados para identificação de uma organização que solicita certificado digital.

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 42, de 18.04.2006 **Versão 2.0**	Diversos	Criação do DOC-ICP-05, consolidando documentos anteriores.

1 INTRODUÇÃO

1.1 Visão geral

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

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

1.1.3 Para as ACs emissoras de certificados SSL e CS, devem ser observados e descritos os princípios e critérios WebTrust.

1.1.4 A estrutura desta DPC está baseada na RFC 3647.

1.1.5 A AC responsável deverá manter todas as informações da sua DPC sempre atualizadas.

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

1.2 Nome do documento e identificação

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

1.2.2 As ACs emissoras de certificados para usuários finais devem ser exclusivas e separadas de acordo com os seguintes propósitos de uso de chaves:

a) autenticação de servidor (SSL/TLS);

b) assinatura de documento e proteção de e-mail (S/MIME);

c) assinatura de código (*Code Signing*); e

d) assinatura de carimbo do tempo (*Timestamping*).

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

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

1.3.2 Autoridades de Registro

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

a) relação de todas as ARs credenciadas;

b) relação de ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento; e

c) relação de ARs que estejam vinculadas contratualmente a Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, para efeito de emissão de certificado digital de pessoa física em conjunto com a Carteira de Identidade (RG) e a Carteira Nacional de Habilitação (CNH).

1.3.3 Titulares do certificado

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

1.3.4 Partes confiáveis

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

1.3.5 Outros participantes

Neste item deve ser identificado o endereço da página web (URL) onde está publicada a relação de todos os Prestadores de Serviços de Suporte – PSSs, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSCs vinculados à AC responsável.

1.4 Usabilidade do certificado

1.4.1 Uso apropriado do certificado

Este item da DPC deve relacionar e identificar as PCs implementadas pela AC responsável, que definem como os certificados emitidos deverão ser utilizados pela comunidade. Nas PCs estarão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC.

1.4.2 Uso proibitivo do certificado

Este item, quando cabível, deve relacionar as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.5 Política de administração

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 o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC.

1.5.2 Contatos

Endereço:

Telefone:

Fax:

Página web:

E-mail:

Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome:

Telefone:

E-mail:

Outros:

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

1.6 Definições e acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	*Automatic Certificate Management Environment*
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas

CS	*Code Signing*
CSR	*Certificate Signing Request*
DETRAN	Departamento Nacional de Trânsito
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation* (*WebTrust for Certification Authorities*)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*

RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SIGEPE	Sistema de Gestão de Pessoal da Administração Pública Federal
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TLS	*Transport Layer Security*
TSDM	*Trusted Software Development Methodology*
TSE	Tribunal Superior Eleitoral
UF	Unidade de Federação
URL	*Uniform Resource Locator*

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

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

a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e a sua LCR/OCSP;

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

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

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

a) localização física e lógica;

b) disponibilidade;

c) protocolos de acesso; e

d) requisitos de segurança.

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

2.1.4 A AC responsável deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP.

2.2 Publicação de informações dos certificados

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

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

a) seu próprio certificado;

b) suas LCRs/OCSP;

c) sua DPC;

d) as PCs que implementa;

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

f) uma relação, regularmente atualizada, contendo os PSSs, PSBios e PSCs vinculados.

2.3 Tempo ou frequência de publicação

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

2.4 Controle de acesso aos repositórios

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

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Atribuição de nomes

3.1.1 Tipos de nomes

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

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

3.1.2 Necessidade dos nomes serem 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 Anonimato ou pseudônimo dos titulares do certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

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

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

3.1.5 Unicidade de nomes

Neste item a DPC deve estabelecer que identificadores do tipo "*Distinguished Name*" (DN) deverão ser únicos para cada titular de certificado, no âmbito da AC emitente. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 Procedimento para resolver disputa de nomes

Neste item a DPC deve reservar à AC responsável o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes diversos de certificados. Deve estabelecer também que, durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

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

3.2 Validação inicial de identidade

Deverão ser detalhados a forma, os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados digitais, compreendendo os seguintes processos:

a) identificação e cadastro iniciais do titular do certificado – identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7, observado o quanto segue:

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

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

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

3.2.1 Método para comprovar o controle de chave privada

A DPC deve indicar os procedimentos executados pela AC responsável ou pelas ARs a ela vinculadas para confirmar que a entidade solicitante controla a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, podendo utilizar para isso as referências contidas nas RFC 4210 e 6712. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições gerais

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

3.2.2.1.2 Será designado como responsável pelo certificado o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do item 3.2, alínea 'a', inciso (ii) acima, o qual será o detentor da chave privada.

3.2.2.1.3 Deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, nos seguintes termos:

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

b) apresentação do rol de documentos do responsável pelo certificado, elencados no item 3.2.3.1;

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

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

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

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

3.2.2.1.5 O disposto no item 3.2.2.1.3 poderá ser realizado:

a) mediante comparecimento presencial do responsável pelo certificado; ou

b) por videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.2.2.2 Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:

   i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;

   ii. se entidade privada:

      1. certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e

      2. documentos da eleição de seus representantes legais, quando aplicável;

b) Relativos a sua habilitação fiscal:

   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

3.2.2.3 Informações contidas no certificado emitido para uma organização

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

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

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

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

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

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

3.2.2.4 Responsabilidade decorrente do uso do certificado de uma organização

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

---

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

3.2.3 Autenticação da identidade de um indivíduo

Neste item devem ser definidos os procedimentos empregados pelas AR vinculadas a uma AC para a identificação e cadastramento iniciais de um indivíduo na ICP-Brasil. Essa confirmação deverá ser realizada mediante a presença física do interessado ou por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

3.2.3.1 Procedimento para identificação de um indivíduo (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

A identificação da pessoa física requerente do certificado deverá ser realizada como segue: (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

a) apresentação da seguinte documentação, em sua versão original oficial, física ou digital: (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

   i. Registro de Identidade, se brasileiro; ou (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

   ii. Título de Eleitor, com foto; ou (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

   iii. Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

   iv. Passaporte, se estrangeiro não domiciliado no Brasil. (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

b) coleta e verificação biométrica do requerente, conforme regulamentado em Instrução Normativa editada pela AC Raiz, a qual deverá definir os dados biométricos a serem coletados, bem como os procedimentos para coleta e identificação biométrica na ICP-Brasil. (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

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

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

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

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

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

b) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC; e

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

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

3.2.3.1.5 Para a identificação de indivíduo na emissão de certificado digital para servidor público da ativa e militar da União, deverá ser observado o disposto item 3.2.9.3.

3.2.3.1.6 É facultado aos Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo BACEN, na identificação de titulares pessoa física de conta de depósito; às serventias extrajudiciais, autorizadas a funcionar pelo Conselho Nacional de Justiça; às AR dos conselhos de classes profissionais, regulamentados por lei específica; e às ARs com acesso eletrônico às bases de dados das juntas comerciais, utilizar o recurso disposto no item 3.2.9.4.

3.2.3.1.7 Para a identificação de indivíduo na emissão de certificado digital em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverá ser observado o disposto item 3.2.9.8.

3.2.3.1.8 A verificação biométrica do requerente poderá ser realizada por meio de batimento dos dados em base oficial nacional, conforme regulamentado em Instrução Normativa editada pela AC Raiz da ICP-Brasil, que deverá dispor acerca dos procedimentos e das bases oficiais admitidas para tal finalidade. (Redação dada pela Resolução CG ICP-Brasil nº 181, de 2021)

3.2.3.2 Informações contidas no certificado emitido para um indivíduo

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

a) nome completo, sem abreviações;[1]

b) data de nascimento.[2]

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

a) Cadastro de Pessoa Física (CPF);

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

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

d) número do Cadastro Especifico do INSS (CEI);

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

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

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

3.2.3.2.3 Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original.

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

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

3.2.4 Informações não verificadas do titular do certificado

Não se aplica.

3.2.5 Validação das autoridades

Na emissão de certificado de AC subsequente é verificado se a pessoa física é o representante legal da AC.

3.2.6 Critérios para interoperação

Não se aplica.

3.2.7 Autenticação da identidade de equipamento ou aplicação

3.2.7.1 Disposições gerais

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

3.2.7.1.2 Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.2.3 e esta assinará o termo de titularidade de que trata o item 4.1.

3.2.7.1.3 Se o titular for pessoa jurídica, deverá ser feita a confirmação da identidade da organização e da pessoa física responsável pelo certificado, na forma do item 3.2.2:

3.2.7.1.4 Fica dispensada a observância do disposto no item 3.2.3.1 para certificados cujo titular seja pessoa física, caso a solicitação seja assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e cujos dados biométricos já tenham sido devidamente coletados.

3.2.7.1.5 Fica dispensada a observância do item 3.2.2.1.3, alíneas “b” e “c”, para certificados cujo titular seja pessoa jurídica nos seguintes casos:

a) quando a solicitação for assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e responsável, e cujos dados biométricos deste último tenham sido devidamente coletados; ou

b) quando a solicitação for assinada com o certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade é da mesma pessoa física responsável legal da organização e a verificação dos documentos elencados no item 3.2.2.2 possa ser realizada eletronicamente por meio de barramento ou aplicação oficial.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.2.7.2.1 Para certificados de equipamento ou aplicação que utilizem URL na identificação do titular, deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para usar aquele endereço. Nesse caso deve ser apresentada documentação comprobatória (termo de autorização de uso de domínio ou similar) devidamente assinado pelo titular do domínio.

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

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação

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

a) URL ou nome da aplicação;[1]

b) nome completo do responsável pelo certificado, sem abreviações;[2]

c) data de nascimento do responsável pelo certificado;[3]

d) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações[4], se o titular for pessoa jurídica;

e) Cadastro Nacional de Pessoa Jurídica (CNPJ)[5], se o titular for pessoa jurídica.

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

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

3.2.7.4.1 Disposições gerais

3.2.7.4.1.1 Em se tratando de certificado emitido para equipamento SAT, o titular será representado pelo contribuinte identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de série do equipamento detentor da chave privada.

---

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

3.2.7.4.1.2 Para certificados do tipo A CF-e-SAT, a confirmação da identidade da organização e das pessoas físicas se dará conforme disposto no item 3.2.2 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.4.1.3 Para certificados do tipo A CF-e-SAT, por se tratar de certificado para equipamento fiscal específico para contribuinte já identificado quando da emissão do certificado digital ICP-Brasil de pessoa jurídica válido que assina a requisição do certificado A CF-e-SAT, a confirmação da identidade se dará exclusivamente na forma do disposto no item 3.2.3 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT

Para certificados de equipamento SAT, deve ser verificado se o CNPJ do contribuinte que assina digitalmente a solicitação desse certificado está vinculado ao número de série do referido equipamento, o qual deve estar registrado e autorizado pela unidade fiscal federada. Essas informações devem ser obtidas e confirmadas pela AC emissora do certificado.

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT

3.2.7.6.1 É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nas solicitações apresentadas:

a) número de série do equipamento SAT;[1]

b) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;[2]

c) Cadastro Nacional de Pessoa Jurídica (CNPJ).[3]

3.2.7.6.2 Cada PC pode definir como obrigatório o preenchimento de outros campos em conformidade com a RFC 5280 e com a regulamentação SAT CF-e.

3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR

3.2.7.7.1 Disposições gerais

3.2.7.7.1.1 Em se tratando de certificado emitido para equipamento OM-BR, o titular será representado pelo fabricante identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de identificação do equipamento detentor da chave privada.

3.2.7.7.1.2 Para certificados do tipo OM-BR, a confirmação da identidade do fabricante se dará conforme disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.7.1.3 Para certificados do tipo OM-BR, por se tratar de certificado para equipamento metrológico específico de fabricante autorizado já identificado quando da emissão do certificado digital ICP-Brasil de pessoa jurídica válido que assina a requisição do certificado OM-BR, a confirmação da identidade se dará exclusivamente na forma do disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

---

[1] No campo *Subject*, como parte do *Common Name*, que compõe o *Distinguished Name*
[2] No campo *Subject Alternative Name*, OID **2.16.76.1.3.8**
[3] No campo *Subject Alternative Name*, OID **2.16.76.1.3.3**

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico

Para certificados de equipamento metrológico, deve ser verificado se o CNPJ do fabricante que assina digitalmente a solicitação desse certificado está vinculado aos controles regulatórios do referido equipamento, o qual deve estar registrado e autorizado pelo Inmetro. Essas informações devem ser obtidas e confirmadas pela AC emissora do certificado.

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico

3.2.7.9.1 É obrigatório o preenchimento dos seguintes campos do certificado com as informações constantes nas solicitações apresentadas:

a) data de fabricação do equipamento metrológico;

b) número de identificação do equipamento metrológico;

c) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;

d) Cadastro Nacional de Pessoa Jurídica (CNPJ).

3.2.7.9.2 Cada PC pode definir como obrigatório o preenchimento de outros campos em conformidade com a RFC 5280 e com as normas do órgão regulador do equipamento.

3.2.8 Procedimentos complementares

3.2.8.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Requisitos de Linha de Base, as Diretrizes de EV para SSL e as Diretrizes de Assinatura de Código EV.

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

3.2.8.3 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.1 No caso de certificados A CF-e-SAT ou OM-BR deve ser mantida toda a documentação eletrônica utilizada no processo de validação e confirmação da identificação do equipamento SAT ou objeto metrológico acreditado pelo Inmetro, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.2 No caso de certificados emitidos em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverá ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade do indivíduo, incluindo, a Carteira de Identidade ou CNH emitida em conjunto ao certificado. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.4 As AC devem disponibilizar, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6] e em regulamento editado por instrução normativa da AC Raiz que defina os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital ICP-Brasil.

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

3.2.9 Procedimentos específicos

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

3.2.9.2 Disposições para a Validação de Solicitação de Certificados do Tipo A CF-e-SAT: a validação da solicitação de certificado do tipo A CF-e-SAT compreende:

a) validar o registro inicial por meio de verificação da assinatura digital do contribuinte realizada sobre a solicitação do certificado A CF-e-SAT e sobre o TERMO DE TITULARIDADE [4] específico de que trata o item 4.1. O certificado digital do contribuinte que assina a solicitação e o termo de titularidade aqui referidos, deve ser um certificado digital ICP-Brasil de pessoa jurídica válido;

b) realizar a verificação da solicitação, assinada digitalmente, contendo a requisição em conformidade com o formato estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e confrontando com as informações (número de segurança e número de série do equipamento SAT e CNPJ do contribuinte emissor CF-e) do registro inicial e do certificado digital que assinou esse registro inicial;

c) emissão do certificado digital sem que haja possibilidade de alteração dos dados constantes na requisição e disponibilização ao solicitante para instalação no equipamento SAT.

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

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

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

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

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

3.2.9.3.1 Módulo eletrônico da AR dos órgãos gestores de pessoas

A AR, representada pelo módulo eletrônico da AR dos órgãos gestores de pessoas, deverá:

a) ser um sistema vinculado a uma AC credenciada pela ICP-Brasil;

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

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

d) ser auditada pelo ITI em procedimento pré-operacional;

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

Nota: Ficam excepcionalizados para as AR descritas no item 3.2.9.3.1 os requisitos dispostos em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

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

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

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

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

3.2.9.3.3 Aplica-se o disposto no item 3.2.9.3 aos empregados públicos federais de empresas estatais dependentes do orçamento público federal para custeio de pessoal, desde que vinculados ao Sistema de Gestão de Pessoal da Administração Pública Federal – SIGEPE.

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

3.2.9.4 A AR de Bancos Múltiplos ou Caixa Econômica Federal, as serventias extrajudiciais; as ARs dos conselhos de classes profissionais regulamentados por lei específica e em conformidade com a Lei nº 6.206, de 07 de maio de 1975; e as ARs com acesso eletrônico às bases de dados das juntas comerciais, devidamente credenciados na ICP-Brasil, poderão utilizar um módulo eletrônico de AR.

3.2.9.4.1 A AR, representada pelo módulo eletrônico, deverá:

a) ser um sistema vinculado a uma AC credenciada pela ICP-Brasil, de acordo com este normativo;

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

c) comunicar diretamente utilizando protocolos de comunicação seguros com os sistemas determinados formalmente pelos Bancos Múltiplos e Caixa Econômica Federal, pelas serventias extrajudiciais, pelos conselhos de classes profissionais, pelas juntas comerciais, pela AR (quando aplicável), pela AC e pelo Prestador de Serviço Biométrico (PSBio), vedada a utilização de mecanismos intermediários de tratamento de dados;

d) ser auditada pelo ITI em procedimento pré-operacional; e

e) possuir as listas atualizadas com os nomes e CPF dos funcionários autorizados como agentes de registro a verificar as informações de solicitações de certificados por titulares de contas de depósito ou cadastro.

Nota: As AR descritas no item 3.2.9.4 ficam dispensadas dos requisitos dispostos no item "Segurança de Pessoal" e no item "Aplicativo de AR" do regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil, para aqueles requisitos equivalentes aos previstos nas normas do Banco Central do Brasil, do Conselho Nacional de Justiça, dos respectivos conselhos de classes profissionais regulamentados por lei e pelas juntas comerciais.

3.2.9.5 Disposições para a validação de solicitação de certificados do tipo OM-BR:

A validação da solicitação de certificado do tipo OM-BR compreende:

a) validar o registro inicial por meio de verificação da assinatura digital do fabricante do equipamento metrológico realizada sobre a solicitação do certificado OM-BR e sobre o TERMO DE TITULARIDADE [4] específico de que trata o item 4.1. O certificado digital do fabricante que assina a solicitação e o termo de titularidade aqui referidos deve ser um certificado digital ICP-Brasil de pessoa jurídica válido;

b) realizar a verificação da solicitação, assinada digitalmente, contendo a requisição em conformidade com o formato estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e confrontando com as informações de controle do órgão regulador e do certificado digital que assinou a requisição;

c) emissão do certificado digital sem que haja possibilidade de alteração dos dados constantes na requisição e disponibilização ao solicitante para instalação no equipamento OM-BR.

3.2.9.6 Os órgãos e conselhos de classe profissional, a que se refere a Lei n° 6.206, de 7 de maio de 1975, credenciados como AR na ICP-Brasil, poderão realizar a identificação dos profissionais solicitantes sujeitos a registro perante o respectivo órgão ou conselho de classe, por meio de processo de individualização inequívoca realizada através de seus sistemas de emissão da identidade profissional, por agente de registro autorizador, com coleta ou verificação biométrica via PSBio credenciado, pelo recurso disposto no item 3.2.9.4.

3.2.9.7 No caso de solicitação de certificados digitais realizados através do Balcão Único para Abertura de Empresas, as ARs com acesso eletrônico às bases de dados das juntas comerciais, deverão observar o seguinte:

a) o responsável pelo uso do certificado de pessoa jurídica, deverá ser autenticado através de batimento biométrico (1:1) em PSBio credenciado na ICP-Brasil, na base biométrica oficial do TSE ou em outra base biométrica oficial da União, dos Estados ou do Distrito Federal, com comprovação auditável desse processo de autenticação biométrica por parte da AC. Essa comprovação poderá ser pelo CPF ou outro indexador viável entre os sistemas;

b) no caso de impossibilidade da autenticação biométrica por qualquer das formas previstas na alínea ‘b’ acima, deverá ser realizada a identificação biométrica do responsável através do cadastramento biométrico (1:N) junto a PSBio credenciado, conforme as normas vigentes da ICP-Brasil;

c) no caso de a autenticação prevista na alínea ‘b’ ocorrer em base biométrica oficial do TSE ou em outra base biométrica oficial da União, dos Estados ou do Distrito Federal, as biometrias utilizadas deverão ser compartilhadas com a AC, que deverá, em até 7 (sete) dias, submetê-las ao PSBio para cadastramento e batimento biométrico (1:N) ou, caso o responsável já se encontre cadastrado, para o batimento biométrico (1:1) junto à ICP-Brasil, devendo, em qualquer hipótese, ser realizada consulta à Lista Negativa. Em havendo conflito de identificação biométrica detectado pelo PSBio ou ocorrência de registro na Lista Negativa, a AC deverá proceder conforme regulamentado para tais situações;

d) no caso do indivíduo se autenticar por meio de certificado digital de pessoa física ICP-Brasil válido, ficam dispensados os procedimentos previstos nas alíneas ‘b’ e ‘c’ acima;

e) o indivíduo identificado ou autenticado conforme as alíneas anteriores, deverá ser representante legal da pessoa jurídica titular do certificado, conforme conste no registro de abertura de empresa concomitante com a solicitação do respectivo certificado;

f) obter os dados para gerar a requisição do certificado à AC diretamente de seus respectivos sistemas eletrônicos de registro de empresas, sem que haja qualquer possibilidade de alteração desses; e

g) ser assinada por agente de registro devidamente cadastrado no sistema da AC, sendo a AC responsável por manter as respectivas requisições para fins de auditoria e fiscalização pela AC Raiz.

3.2.9.8 No caso de solicitação de certificado a ser emitido em conjunto à Carteira de Identidade (RG) ou à Carteira Nacional de Habilitação (CNH), por Órgão de Identificação ou Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, deverão ser observados os seguintes requisitos:

a) a pessoa física titular do certificado deverá ter sido biometricamente identificado e individualizado na base biométrica do órgão responsável pela emissão da Carteira de Identidade (RG) ou da Carteira Nacional de Habilitação (CNH), conforme o caso, bem como ter dado consentimento expresso e específico para o compartilhamento com as entidades da ICP-Brasil dos dados biométricos e biográficos necessários para a identificação, cadastro e emissão do certificado digital. Essa individualização poderá ser pelo CPF ou outro indexador viável entre os sistemas;

b) as biometrias e os dados biográficos necessários para emissão dos certificados, previstos no DOC ICP 04, deverão ser compartilhados com a AC/AR, com base nos quais a AR fará a identificação e cadastro na ICP Brasil, através do sistema eletrônico da AC;

c) a AC/AR deverá submetê-las ao PSBio para cadastramento e batimento biométrico (1:N), ou no caso de indivíduo já cadastrado, para o batimento biométrico (1:1) junto à ICP-Brasil, e também para consulta à Lista Negativa. Em havendo conflito de identificação biométrica detectado pelo PSBio ou ocorrência de registro na Lista Negativa, a AC/AR deverá proceder conforme regulamentado para tais situações; e

d) não havendo conflito de identificação biométrica detectado pelo PSBio ou ocorrência de registro na Lista Negativa, a AC contratada deverá emitir o certificado digital na modalidade em Prestador de Serviço de Confiança (PSC) de armazenamento de chaves criptográficas, sem que haja possibilidade de alteração dos dados constantes da Carteira de Identidade (RG) ou da Carteira Nacional de Habilitação (CNH), habilitando o uso de chaves somente após o batimento biométrico (1:1) ou após conclusão do cadastramento biométrico.

3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 Neste item a DPC deve estabelecer os processos de identificação e confirmação do cadastro do solicitante, utilizados pela AC responsável para a geração de novo par de chaves e de seu correspondente novo certificado.

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

a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2, 3.2.3 ou 3.2.7;

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

c) solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido de uma organização, do tipo A3 ou superior, para o qual tenham sido coletados os dados biométricos do responsável pelo certificado, desde que, mantido nessa condição, apresente documento digital verificável por meio de barramento ou aplicação oficial dos entes federativos, que comprove poder de representação legal em relação à organização, permitida tal hipótese apenas para os certificados digitais de organizações;

d) solicitação por meio eletrônico dada nas alíneas 'b' e 'c' acima, conforme o caso, para certificado ICP-Brasil válido do tipo A1, que seja do mesmo nível de segurança, mediante confirmação do respectivo cadastro, por meio de videoconferência, conforme regulamentação a ser editada pela AC Raiz, ou limitada a 1 (uma) ocorrência sucessiva quando não tiverem sido colhidos os dados biométricos do titular ou responsável;

e) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz, os quais deverão assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou

f) por meio de mecanismo automatizado de gerenciamento de certificado do tipo SSL/TLS (ACME), conforme disposto no item 3.3.2.1.

3.3.2.1 Para certificados de equipamento ou aplicação que utilizem URL, a AC poderá implementar mecanismos automatizado de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e a identificação do solicitante, seja pessoa física ou jurídica. O processo automatizado implica as seguintes etapas:

a) o solicitante submete uma requisição de certificado (PKCS#10) da URL desejada;

b) a requisição deverá ser acompanhada do certificado da URL solicitada, ainda válido, e o conjunto (requisição + certificado da URL) deve ser assinado com certificado ICP-Brasil, no mínimo do tipo A3, de pessoa física ou jurídica do responsável pelo domínio. Se o responsável pelo domínio for pessoa física, o signatário deve ser o mesmo contido no campo otherName (OID 2.16.76.1.3.2) que identifica o responsável pelo certificado da URL. Se o responsável pelo domínio for pessoa jurídica, o signatário deve ser um certificado de pessoa jurídica cujo CNPJ seja o mesmo contido no campo otherName (OID 2.16.76.1.3.3) que identifica o titular do certificado da URL;

c) o aplicativo de AR valida a assinatura e a requisição e, caso esteja em conformidade, encaminha desafio de prova de domínio e o termo de titularidade;

d) o solicitante responde o desafio e assina o termo de titularidade com o mesmo certificado utilizado no item "b", acima;

e) confirmado atendimento pleno do desafio e da assinatura do termo de titularidade, o aplicativo de AR poderá emitir o certificado e encaminhá-lo ao solicitante; e

f) todas as evidências do processo acima devem constar no dossiê do certificado.

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

3.3.4 Para os casos específicos de expiração ou revogação de um certificado de AC de nível imediatamente subsequente ao da AC responsável pela DPC, este item deve estabelecer que, após a expiração ou revogação de seu certificado, aquela AC deverá executar os processos regulares de geração de seu novo par de chaves.

3.4 Identificação e autenticação para solicitação de revogação

O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.9.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Raiz.

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

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

Neste item da DPC devem ser descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC responsável e pelas ARs a ela vinculadas para as solicitações de emissão de certificado. Esses requisitos e procedimentos deverão compreender, em detalhes, todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital. A descrição deve ainda contemplar:

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

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

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

Nota 1: o termo de titularidade para certificados de usuários finais com propósito de uso EV SSL e EV CS deve seguir o padrão adotado no documento EV SSL e EV CS Guidelines.

Nota 2: na impossibilidade técnica de assinatura digital do termo de titularidade (como certificados SSL, de equipamento, aplicação, codesign, carimbo de tempo e outros que façam uso de CSR) será aceita a assinatura manuscrita do termo ou assinatura digital do termo com o certificado ICP-Brasil do titular do certificado ou responsável pelo certificado, no caso de certificado de pessoa jurídica. No caso de assinatura manuscrita do termo será necessária a verificação da assinatura contra o documento de identificação.

4.1.1 Quem pode submeter uma solicitação de certificado

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

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

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

4.1.1.3 Nos casos previstos no item 4.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

4.1.1.4 A DPC deve observar que a solicitação de um certificado de AC de nível imediatamente subsequente deve ser feita pelos seus representantes legais.

4.1.2 Processo de registro e responsabilidades

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

4.1.2.1 Responsabilidades da AC

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

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

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

4.1.2.2 Obrigações da AC

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

a) operar de acordo com a sua DPC e com as PCs que implementa;

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

c) assegurar a proteção de suas chaves privadas;

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

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

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu ou os certificados de AR a ela vinculadas e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

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

k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;

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

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

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

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

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

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

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

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

t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

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

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

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

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

4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4 Obrigações das ARs

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

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

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

c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;

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

e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil, bem como Princípios e Critérios WebTrust para AR [5];

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

g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2, 3.2.3 e 3.2.7; e

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

4.2 Processamento de solicitação de certificado

4.2.1 Execução das funções de identificação e autenticação

A AC e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.2.1 A AC pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 4.1 desta DPC.

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

4.2.3 Tempo para processar a solicitação de certificado

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

4.3 Emissão de certificado

4.3.1 Ações da AC durante a emissão de um certificado

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

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

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

Após a emissão do certificado, a AC deve descrever a forma de notificação ao titular do certificado sobre sua emissão.

4.4 Aceitação de certificado

4.4.1 Conduta sobre a aceitação do certificado

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

4.4.1.2 A DPC deve garantir que a aceitação de todo certificado emitido seja declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

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

4.4.2 Publicação do certificado pela AC

O certificado da AC e os certificados das ACs de nível imediatamente subsequente ao seu são publicados de acordo com item 2.2 desta DPC.

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

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

4.5 Usabilidade do par de chaves e do certificado

A AC subsequente titular de certificado emitido pela AC ou o titular do certificado para usuário final devem operar de acordo com a sua própria Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) que implementar, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.1.1 A AC titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto na sua própria DPC.

4.5.1.2 Obrigações do Titular do Certificado

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos pela AC responsável pela DPC, constantes dos termos de titularidade de que trata o item 4.1, devendo incluir no mínimo os itens abaixo relacionados:

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

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

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

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

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

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

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6 Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6 Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7 Nova chave de certificado (Re-key)

4.7.1 Circunstâncias para nova chave de certificado

Não se aplica

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

Não se aplica

4.7.3 Processamento de requisição de novas chaves de certificado

Não se aplica

4.7.4 Notificação de emissão de novo certificado para o titular

Não se aplica

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica

4.7.6 Publicação de uma nova chave certificada pela AC

Não se aplica

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

Não se aplica

4.8 Modificação de certificado

Não se aplica

4.8.1 Circunstâncias para modificação de certificado

Não se aplica

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica

4.8.3 Processamento de requisição de modificação de certificado

Não se aplica

4.8.4 Notificação de emissão de novo certificado para o titular

Não se aplica

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica

4.8.6 Publicação de uma modificação de certificado pela AC

Não se aplica

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

Não se aplica

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

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

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

a) Quando constatada emissão imprópria ou defeituosa do mesmo;

b) Quando for necessária a alteração de qualquer informação constante no mesmo;

c) No caso de dissolução de AC titular do certificado; ou

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

4.9.1.3 A DPC deve observar ainda que:

a) A AC emitente deverá revogar, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e

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

4.9.1.4 A DPC deve observar que todo certificado deverá ter a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.9.1.4.1 ACs que emitem certificados SSL e CS devem suportar requisições OCSP em conformidade com a RFC 6960 e/ou RFC5019 e requisitos WebTrust. Para certificados SSL e CS, a resposta OCSP deve ter validade mínima de um dia e máxima de uma semana, sendo que a próxima atualização deve estar disponível a cada quatro dias.

4.9.1.4.2 ACs que emitem certificados SSL e CS devem prover garantias que uma LCR pode ser baixada em não mais do que três segundos por uma linha de telefone analógica, sobre uma condição normal de rede.

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

4.9.2 Quem pode solicitar revogação

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

a) Por solicitação do titular do certificado;

b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;

c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;

d) Pela AC emitente;

e) Por uma AR vinculada;

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

g) Pela unidade fiscal federada do contribuinte, quando tratar-se de certificado do tipo A CF-e-SAT;

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

i) Pelo Inmetro, quando se tratar de certificado do tipo OM-BR; ou

j) Por funcionário ou colaborador contratado de Órgão de Identificação ou de Departamento de Trânsito (Detran), dos Estados e do Distrito Federal, formalmente autorizado por autoridade competente, quando se tratar de certificado emitido em conjunto com a Carteira de Identidade (RG) ou a Carteira Nacional de Habilitação (CNH).

4.9.3 Procedimento para solicitação de revogação.

4.9.3.1 Neste item da DPC devem ser descritos os procedimentos estabelecidos pela AC para a solicitação de revogação de certificados. A AC deverá garantir que todos agentes habilitados, conforme o item 4.9.2, possam, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados. Caso sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos devem ser descritos nessas PCs, no item correspondente.

4.9.3.2 Como diretrizes gerais, a DPC deve estabelecer que:

a) O solicitante da revogação de um certificado será identificado;

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

c) As justificativas para a revogação de um certificado serão documentadas; e

d) O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC.

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

4.9.3.4 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.

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

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

4.9.4 Prazo para solicitação de revogação

4.9.4.1 Neste item, a DPC deve observar que a solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no seu item 4.9.1 e deve estabelecer o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado poderá ser solicitada sem cobrança de tarifa pela AC.

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

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

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

4.9.7.1 Neste item deve ser definida a frequência de emissão da LCR referente a certificados de usuários finais e de AC de nível imediatamente subsequente ao da AC responsável.

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

4.9.7.3 A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC responsável deverá emitir nova LCR no prazo previsto no item 4.9.3.4 e notificar todas as ACs de nível imediatamente subsequente ao seu.

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

4.9.7.5 Para certificados EV SSL e EV CS as frequências de emissão de LCR devem ser implementadas e descritas em suas PCs, no item correspondente, em conformidade com os requisitos Webtrust.

4.9.8 Latência máxima para a LCR

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

4.9.9 Disponibilidade para revogação/verificação de status on-line

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

4.9.10 Requisitos para verificação de revogação on-line

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

4.9.11 Outras formas disponíveis para divulgação de revogação

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

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

4.9.12 Requisitos especiais para o caso de comprometimento de chave

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

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

4.9.13 Circunstâncias para suspensão

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

4.9.14 Quem pode solicitar suspensão

A AC, aprovados pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão dados por norma específica das DPC e PCs associadas.

4.9.16 Limites no período de suspensão

Os períodos de suspensão serão estabelecidos por norma específica das DPC e PCs associadas.

4.10 Serviços de status de certificado

4.10.1 Características operacionais

A AC deve fornecer um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificado ou OCSP, conforme item 4.9.

4.10.2 Disponibilidade dos serviços

Ver item 4.9.

4.10.3 Funcionalidades operacionais

Ver item 4.9.

4.11 Encerramento de atividades

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

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

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

Neste item deve ser descrito os procedimentos de custódia (*escrow*) e práticas e políticas de recuperação de chaves privadas de sigilo da AC.

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

Neste item deve ser identificado o documento ou lista contendo as políticas e práticas de encapsulamento e recuperação de chave de sessão na AC.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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

5.1 Controles físicos

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

5.1.1 Construção e localização das instalações de AC

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

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

a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;

b) Instalações para sistemas de telecomunicações;

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

d) Iluminação de emergência.

5.1.2 Acesso físico

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

5.1.2.1 Níveis de acesso

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

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

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

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

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

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

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

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

5.1.2.1.9 No quarto nível, todas as paredes, piso e teto deverão ser revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto deverão ser inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não deverão permitir a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre – deverão possuir proteção contra interferência eletromagnética externa.

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

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

a) Equipamentos de produção *on-line* e cofre de armazenamento;

b) Equipamentos de produção *off-line* e cofre de armazenamento; e

c) Equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores).

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

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

a) Ser feito em aço ou material de resistência equivalente; e

b) Possuir tranca com chave.

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

5.1.2.2 Sistemas físicos de detecção

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

5.1.2.2.2 As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 7 (sete) anos. Elas deverão ser testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas deverão ser armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente deverão ser monitoradas por sistema de notificação de alarmes. Onde houver, a partir do nível 2, vidros separando níveis de acesso, deverá ser implantado um mecanismo de alarme de quebra de vidros, que deverá estar ligado ininterruptamente.

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

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

5.1.2.2.6 O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, deverão ser permanentemente monitorados 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.

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1 Mecanismos específicos deverão ser implantados pela AC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

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

5.1.3 Energia e ar-condicionado

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

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

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

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

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

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

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

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

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

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

a) Geradores de porte compatível;

b) Geradores de reserva;

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

d) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5.1 Os sistemas de prevenção contra incêndios, internos aos ambientes, deverão possibilitar alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

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

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

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

5.1.6 Armazenamento de mídia

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

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

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

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

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

5.2 Controles Procedimentais

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

5.2.1 Perfis qualificados

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

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

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

5.2.1.3.1 A AC deve realizar um exame, para emissão de certificados em cadeia do tipo SSL e CS, nos operadores do sistema de certificação da AC, de acordo com os requisitos de princípios e critérios *WebTrust Baseline*.

5.2.1.4 Quando um empregado se desligar da AC, suas permissões de acesso deverão ser revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC, deverão ser revistas suas permissões de acesso. Deverá existir uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 A DPC deve estabelecer o requisito de controle multiusuário para a geração e a utilização da chave privada da AC responsável, na forma definida no item 6.2.2.

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

5.2.3 Identificação e autenticação para cada perfil

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

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

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

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

d) Receber uma conta no sistema de certificação da AC.

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

a) Ser diretamente atribuídos a um único empregado;

b) Não ser compartilhados; e

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

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

5.2.4 Funções que requerem separação de deveres

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

5.3 Controles de Pessoal

Nos itens seguintes da DPC devem ser descritos requisitos e procedimentos, implementados pela AC responsável, pelas ARs e PSSs vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. A DPC deve garantir que todos os empregados da AC responsável e das ARs e PSSs vinculados, encarregados de tarefas operacionais terão registrado em contrato ou termo de responsabilidade:

a) Os termos e as condições do perfil que ocuparão;

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

c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

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

5.3.2 Procedimentos de verificação de antecedentes

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

a) Verificação de antecedentes criminais;

b) Verificação de situação de crédito;

c) Verificação de histórico de empregos anteriores; e

d) Comprovação de escolaridade e de residência.

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

5.3.3 Requisitos de treinamento

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

a) Princípios e mecanismos de segurança da AC e das ARs vinculadas;

b) Sistema de certificação em uso na AC;

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

d) Reconhecimento de assinaturas e da validade dos documentos apresentados, na forma dos itens 3.2.2 e 3.2.3 e 3.2.7; e

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

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

5.3.5 Frequência e sequência de rodízio de cargos

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

5.3.6 Sanções para ações não autorizadas

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

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

a) Relato da ocorrência com "*modus operandis*";

b) Identificação dos envolvidos;

c) Eventuais prejuízos causados;

d) Punições aplicadas, se for o caso; e

e) Conclusões.

5.3.6.3 Concluído o processo administrativo, a AC responsável deverá encaminhar suas conclusões à AC Raiz.

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

a) Advertência;

b) Suspensão por prazo determinado; ou

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

5.3.7 Requisitos para contratação de pessoal

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

5.3.8 Documentação fornecida ao pessoal

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

a) Sua DPC;

b) As PCs que implementa;

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

d) Documentação operacional relativa a suas atividades; e

e) Contratos, normas e políticas relevantes para suas atividades.

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

5.4 Procedimentos de Log de Auditoria

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.

5.4.1 Tipos de eventos registrados

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

a) Iniciação e desligamento do sistema de certificação;

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

c) Mudanças na configuração da AC ou nas suas chaves;

d) Mudanças nas políticas de criação de certificados;

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

f) Tentativas não-autorizadas de acesso aos arquivos de sistema;

g) Geração de chaves próprias da AC ou de chaves de seus usuários finais;

h) Emissão e revogação de certificados;

i) Geração de LCR;

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

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

l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1 A AC, emissora de certificados SSL e CS, deve ter capacidade de auditar esses tipos certificados em até seis por cento dos emitidos.

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

a) Registros de acessos físicos;

b) Manutenção e mudanças na configuração de seus sistemas;

c) Mudanças de pessoal e de perfis qualificados;

d) Relatórios de discrepância e comprometimento; e

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

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

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

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

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

a) Os agentes de registro que realizaram as operações;

b) Data e hora das operações;

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

d) A assinatura digital do executante.

5.4.1.7 A AC a que esteja vinculada a AR deve definir, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2 Frequência de auditoria de registros

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.

5.4.3 Período de retenção para registros 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, subsequentemente, deverá armazená-los da maneira descrita no item 5.5.

5.4.4 Proteção de registros de auditoria

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

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

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

5.4.5 Procedimentos para cópia de segurança (Backup) de registros 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.

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

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

5.4.7 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.

5.4.8 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.

5.5 Arquivamento de Registros

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

5.5.1 Tipos de registros arquivados

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

a) Solicitações de certificados;

b) Solicitações de revogação de certificados;

c) Notificações de comprometimento de chaves privadas;

d) Emissões e revogações de certificados;

e) Emissões de LCR;

f) Trocas de chaves criptográficas da AC responsável; e

g) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

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

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;

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

c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.

5.5.3 Proteção de arquivo

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

5.5.4 Procedimentos de cópia de arquivo

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

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

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

5.5.5 Requisitos para datação de registros

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

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

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

5.5.7 Procedimentos para obter e verificar informação de arquivo

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

5.6 Troca de chave

5.6.1 Neste item, a DPC deve descrever os procedimentos para o fornecimento, pela AC responsável, de um novo certificado, antes da expiração do certificado ainda válido do mesmo titular e definir o prazo anterior à data de expiração do certificado, no qual a AC ou uma AR vinculada comunicará ao seu titular para que seja solicitada a emissão de um novo certificado.

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

5.7 Comprometimento e Recuperação de Desastre

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

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

5.7.1.1 A AC deve possuir um Plano de Continuidade do Negócio – PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.

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

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

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

c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;

d) Documentação dos processos e procedimentos acordados;

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

f) Teste e atualização dos planos.

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

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.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 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.

5.7.3.2 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.

5.7.4 Capacidade de continuidade de negócio após desastre

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.

5.8 Extinção da AC

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1 Neste item, a DPC deve descrever os requisitos e procedimentos referentes ao processo de geração do par de chaves criptográficas da AC responsável. O par de chaves criptográficas da AC responsável pela DPC deverá ser gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

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

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

6.1.1.4 A DPC deve indicar que o processo de geração do par de chaves da AC responsável é feito por hardware.

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

6.1.1.6 A DPC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC responsável. Poderão ser indicados padrões de referência, como aqueles definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade

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

6.1.3 Entrega da chave pública para emissor de certificado

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

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

6.1.4 Entrega de chave pública da AC às terceiras partes

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 e terceiras partes, as quais poderão compreender, entre outras:

a) No momento da disponibilização de um certificado para seu titular; usando formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil;

b) Diretório;

c) Página web da AC; e

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

6.1.5 Tamanhos de chave

6.1.5.1 Neste item, a DPC deve observar que cada PC implementada pela AC responsável definirá o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2 Caso a AC responsável emita certificados para outras ACs, neste item deve ser também informado o tamanho das chaves criptográficas associadas a esses certificados, observado o disposto em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

6.1.6.1 A DPC deve prever que os parâmetros de geração de chaves assimétricas da AC responsável adotarão o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6.2 Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

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

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

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

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

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

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 A DPC deve prever que o módulo criptográfico de geração de chaves assimétricas da AC responsável adotará o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.1.2 A DPC deve também, quando cabível, especificar os padrões - como, por exemplo, aqueles definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil - requeridos para os módulos de geração de chaves criptográficas dos titulares de certificado. Cada PC implementada deve especificar os requisitos adicionais aplicáveis.

6.2.2 Controle “n de m” para chave privada

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

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

6.2.3 Custódia (*escrow*) de chave privada

Neste item a DPC deve identificar quem é o agente de recuperação (*escrow*), qual forma que a chave é recuperada (por exemplo, inclui o texto em claro, encriptado, por divisão de chaves) e quais são os controles de segurança do sistema de recuperação.

6.2.4 Cópia de segurança de chave privada

6.2.4.1 A DPC deve observar que, como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

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

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

6.2.4.4 Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos 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

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

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

6.2.6 Inserção de chave privada em módulo criptográfico

Neste item da DPC, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada da AC responsável em módulo criptográfico. A RFC 4210 e 6712 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 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 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.

6.2.9 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.

6.2.10 Método de destruição de chave privada

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

6.3 Outros aspectos do gerenciamento do par de chaves

6.3.1 Arquivamento de chave pública

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

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

6.3.2.1 As chaves privadas da AC responsável pela DPC e dos titulares de certificados de assinatura digital por ela emitidos deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

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

6.3.2.3 Cada PC implementada pela AC responsável deve definir o período máximo de validade do certificado que define, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4 A validade admitida para certificados de AC é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4 Dados de ativação

Nos itens seguintes da DPC, devem ser descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada deve descrever os requisitos específicos aplicáveis.

6.4.1 Geração e instalação dos dados de ativação

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

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

6.4.2 Proteção dos dados de ativação

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

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

6.4.3 Outros aspectos dos dados de ativação

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

6.5 Controles de segurança computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

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

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

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

a) Controle de acesso aos serviços e perfis da AC;

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

c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

d) Geração e armazenamento de registros de auditoria da AC;

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

f) Mecanismos para cópias de segurança (*backup*).

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

6.5.1.5 Qualquer equipamento, ou parte deste, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC. Todos esses eventos deverão ser registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

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

6.5.3 Controles de Segurança para as Autoridades de Registro

6.5.3.1 Neste item, a DPC deve descrever os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas ARs para os processos de validação e aprovação de certificados.

6.5.3.2 Devem ser incluídos, pelo menos, os requisitos especificados em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

6.6 Controles técnicos do ciclo de vida

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

6.6.1 Controles de desenvolvimento de sistema

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

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

6.6.2 Controles de gerenciamento de segurança

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

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

6.6.3 Controles de segurança de ciclo de vida

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

6.6.4 Controles na geração de LCR

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

6.7 Controles de segurança de rede

6.7.1 Diretrizes Gerais

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

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

6.7.1.3 Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC, deverão estar localizados e operar em ambiente de nível, no mínimo, 4.

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

6.7.1.5 O acesso lógico aos elementos de infraestrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2 Firewall

6.7.2.1 Mecanismos de *firewall* deverão ser implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Um *firewall* deverá promover o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC.

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O sistema de detecção de intrusão deverá ter capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.7.3.2 O sistema de detecção de intrusão deverá ter capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.7.3.3 O sistema de detecção de intrusão deverá prover o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência 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 Carimbo de Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[9].

7 PERFIS DE CERTIFICADO, LCR E OCSP

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, de acordo com o perfil estabelecido na RFC 5280. O conteúdo e perfis dos certificados emitidos nas cadeias EV SSL e EV CS devem seguir os estabelecidos nos documentos EV SSL e EV CS Guidelines.

7.1.1 Número de versão

Todos os certificados emitidos pela AC responsável deverão implementar a versão 3.

7.1.2 Extensões de certificado

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

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

b) "***Subject Key Identifier***", **não crítica**: deve conter o *hash* SHA-1 da chave pública da AC titular do certificado;

c) "***Key Usage***", **crítica**: somente os bits keyCertSign e cRLSign devem estar ativados;

d) "**Certificate Policies**", **não crítica**:

d.1) o campo policyIdentifier deve conter:

i. o OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs; ou

ii. os OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;

d.2) o campo **policyQualifiers** deve conter o endereço Web da DPC da AC que emite o certificado;

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

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

7.1.3 Identificadores de algoritmo

Os certificados de AC deverão ser assinados com o uso do algoritmo definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4 Formatos de nome

7.1.4.1 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

OU = nome da AC emitente

CN = nome da AC titular

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

7.1.6 OID (Object Identifier) da 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 5280, em certificados emitidos pela AC responsável para outras ACs.

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 as extensões críticas de PC

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número(s) de versão

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

7.2.2 Extensões de LCR e de suas entradas

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

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

a) "***Authority Key Identifier***": deve conter o *hash* SHA-1 da chave pública da AC que assina a LCR; e

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

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

Serviços de respostas OCSP deverão implementar a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2 Extensões de OCSP

Se implementado, deve estar em conformidade com a RFC 6960.

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

8.2 Identificação/Qualificação do avaliador

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

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

8.3 Relação do avaliador com a entidade avaliada

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

8.4 Tópicos cobertos pela avaliação

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

8.4.2 Neste item da DPC, a AC responsável deve informar que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

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

8.5 Ações tomadas como resultado de uma deficiência

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

8.6 Comunicação dos resultados

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

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 Tarifas

9.1.1 Tarifas de emissão e renovação de certificados

As tarifas de emissão e de renovação de certificado pela AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [1].

9.1.2 Tarifas de acesso ao certificado

Não se aplica.

9.1.3 Tarifas de revogação ou de acesso à informação de status

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

9.1.4 Tarifas para outros serviços

Tarifas para outros serviços da AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [1].

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

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

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

9.3.2 Informações fora do escopo de informações confidenciais

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

a) os certificados e as LCRs/OCSP emitidos pela AC;

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

c) as PCs implementadas pela AC;

d) a DPC da AC;

e) versões públicas de PS; e

f) a conclusão dos relatórios de auditoria.

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

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

a) qualquer PC aplicável;

b) qualquer DPC;

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

d) a conclusão dos relatórios da auditoria.

9.3.2.3 A AC também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1 Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

9.3.3.2 A chave privada de assinatura digital da AC 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.

9.3.3.3 A DPC deve informar que os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

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

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de informação como privadas

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

9.4.3 Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais e de AC de nível imediatamente subsequente ao da AC são fornecidas na LCR/OCSP da AC.

9.4.4 Responsabilidade para proteger a informação privadas

A AC e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas

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

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

Autorizações formais podem ser apresentadas de duas formas:

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

b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

As informações privadas ou confidenciais sob a guarda da AC poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8 Informações a terceiros

Este item da DPC deve estabelecer como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC responsável pela DPC deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

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

9.6.1.3 Identificação do requerente

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

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

A AC mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios, das ACs subsequentes e LCRs/OCSP.

9.6.1.6 Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil e nos documentos *Baseline Requirements*, *EV SSL Guidelines* e/ou *EV CS Guidelines*.

9.6.1.7 Existência legal

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

9.6.2 Declarações e garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

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

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1 As terceiras partes devem:

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

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

9.6.4.2 O certificado da AC ou um certificado de AC de nível imediatamente subsequente ao da AC é considerado válido quando:

i. tiver sido emitido pela AC;

ii. não constar como revogado pela AC;

iii. não estiver expirado; e

iv. puder ser verificado com o uso do certificado válido da AC.

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

9.6.5 Representações e garantias de outros participantes

Não se aplica.

9.7 Isenção de garantias

Não se aplica.

9.8 Limitações de responsabilidades

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

9.9 Indenizações

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

9.10 Prazo e rescisão

9.10.1 Prazo

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

9.10.2 Término

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

9.10.3 Efeito da rescisão e sobrevivência

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

9.11 Avisos individuais e comunicações com os participantes

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

9.12 Alterações

9.12.1 Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida para AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no site da AC.

9.12.3 Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13 Solução de conflitos

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

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

9.14 Lei aplicável

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

9.15 Conformidade com a Lei aplicável

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

9.16 Disposições Diversas

9.16.1 Acordo completo

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

9.16.2 Cessão

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

9.16.3 Independência de disposições

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

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17 Outras provisões

Não se aplica.

10 DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003	**DOC-ICP-09**
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003	**DOC-ICP-08**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001	**DOC-ICP-03**
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	**DOC-ICP-04**
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	**DOC-ICP-02**
[9]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008	**DOC-ICP-12**
[1]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL Aprovado pela Resolução nº 10, de 14 de fevereiro de 2002	**DOC-ICP-06**

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[4]	TERMOS DE TITULARIDADE	**ADE-ICP-05.B**

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

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

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

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

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, september 2007

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

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.