RESOLUÇÃO CG ICP-BRASIL N° 192, DE 16 DE NOVEMBRO DE 2021

Aprova a versão revisada e consolidada do documento Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil – DOC-ICP-01.

O COORDENADOR SUBSTITUTO 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 reunião ordinária, realizada em sessão por videoconferência em 16 de novembro de 2021,

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,

RESOLVEU:

Art. 1° Esta Resolução aprova a versão revisada e consolidada do documento Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.

Art. 2° Fica aprovada a versão 6.0 do documento DOC-ICP-01 – Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.

Art. 3° Ficam revogadas:

I - a Resolução n° 49, de 03 de junho de 2008;

II - a Resolução n° 50, de 28 de novembro de 2008;

III - a Resolução n° 81, de 17 de junho de 2010;

IV - a Resolução n° 94, de 27 de setembro de 2012;

V - a Resolução n° 99, de 09 de outubro de 2013;

VI - a Resolução n° 104, de 23 de abril de 2015;

VII - a Resolução n° 116, de 09 de dezembro de 2015;

VIII - a Resolução n° 143, de 06 de setembro de 2018;

IX - a Resolução n° 147, de 07 de novembro de 2018;

X - a Resolução n° 151, de 30 de maio de 2019;

XI - a Resolução n° 152, de 13 de agosto de 2019; e

XII - a Resolução n° 165, de 17 de abril de 2020.

Art. 4° Esta Resolução entra em vigor em 1° de dezembro de 2021.

ORLANDO OLIVEIRA DOS SANTOS

Infraestrutura de Chaves Públicas Brasileira

ANEXO

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL

DOC-ICP-01

Versão 6.0

16 de novembro 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 192, de 16.11.2021 Versão 6.0		Revisão e consolidação conforme o Decreto nº 10.139, de 28 de novembro de 2019.
Resolução nº 165, de 17.04.2020 Versão 5.2	7.1.2.2	Permitir a configuração de bits específicos nas extensões dos certificados EV.
Resolução nº 152, de 13.08.2019 Versão 5.1	1.1, 4.2 e 10.4 (incluído)	Ajustes aos princípios e critérios WebTrust que referencia requisitos do CABForum.
Resolução nº 151, de 30.05.2019 Versão 5.0		Aprova a versão 5.0 do DOC-ICP-01.
Resolução nº 147, de 07.11.2018 Versão 4.7	7.1.2, 7.1.4	Autoriza revogação das cadeias V8 e V9 e a emissão das cadeias V10 e V11
Resolução nº 143, de 06.09.2018 Versão 4.6	7.1.2 e 7.1.4	Inclusão das cadeias V6, V7, V8 e V9.
Resolução nº 116, de 09.12.2015 Versão 4.5	4.4.3.3, 4.4.9, 7.1.2, alínea c) e 7.1.4, alínea f)	Inclusão da cadeia V5, Revogação de certificados pela AC Raiz, LCR final e flexibilização da frequência de emissão da LCR da AC Raiz.
Resolução nº 104, de 23.04.2015 Versão 4.4	7.1.2, item c) 7.1.4, item e)	Inclusão da cadeia V4
Resolução nº 99, de 09.10.2013 Versão 4.3	7.1	Item alterado que amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 94, de 27.09.2012 Versão 4.2	1.3.3, 1.4, 7.2, 7.2.2, 7.2.2.1, 7.2.2.2, 7.2.6, 7.2.7, 7.2.8, 7.2.8.1, 7.2.8.2, 7.2.9	Itens alterados ou incluídos em função de mudança do prestador de Serviço de Suporte, alterações nos Dados de Contato e detalhamento de Perfil de Certificado.
Ato nº 01, de 26.08.2011 mantida versão 4.1	7.2	Item alterado para corrigir erro de redação
Resolução nº 81, de 17.06.2010 Versão 4.1	7.1.2, 7.1.4, 7.2.4	Inclusão das cadeias V2 e V3
Resolução nº 50, de 19.11.2008 Versão 4.0	2.1.1.g, 2.7.1, 2.8.2.2, 2.8.2.3, 6.1.4.2.c	Inclusão de referências a Carimbo de tempo
Resolução nº 49, de 03.06.08 Versão 3.0	1.1.1, 1.1.2, 2.1.1, 2.1.4.2, 2.6.1.1, 2.6.3.1, 2.8.3, 4.4.1.4, 4.4.1.5, 4.4.1.7, 4.4.9, 4.4.10, 5.2.1.6, 6.1.1.1, 6.1.1.3, 6.1.8, 6.1.9, 6.2, 6.2.1, 6.2.2, 6.2.4.1, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.3.2, 6.4.1, 6.4.2, 6.5.1.1, 6.6.2, 6.7, 6.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.3, 7.3.1, 7.3.2	Item alterado ou excluído em função da geração da segunda chave da AC Raiz
	2.6.1.4, 3.1.1, 5.3.3, 5.3.8, 6.3.1	Item alterado ou excluído para correção de redação
	3.1.7	Item alterado para atualização de padrão internacional
	7.2.2	Item alterado para ficar em conformidade com o padrão internacional

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 46, de 03.12.2007 Versão 2.1	2.6.1.1	Alterada a URL da página Web da AC Raiz para http://acraiz.icpbrasil.gov.br
Resolução nº 38, de 18.04.2006 Versão 2.0	Diversos	Criação do DOC-ICP-01 consolidando documentos anteriores

1 INTRODUÇÃO

1.1 Visão geral

1.1.1 A ICP-Brasil é uma plataforma criptográfica de confiança que garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos por essa infraestrutura.

1.1.2 Este documento é aprovado pelo Comitê Gestor da ICP-Brasil para identificar as práticas e procedimentos da AC Raiz.

1.1.3 Esta Declaração de Práticas de Certificação - DPC descreve as práticas e os procedimentos empregados pelo Instituto Nacional de Tecnologia da Informação - ITI na execução dos seus serviços como Autoridade Certificadora Raiz – AC Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

1.1.4 A AC Raiz possui os certificados de níveis mais altos na ICP-Brasil. Esses certificados contém as chaves públicas correspondentes às chaves privadas da AC Raiz, utilizadas para assinar os seus próprios certificados, os certificados das ACs de nível imediatamente subsequente ao seu e as suas Listas de Certificados Revogados - LCR.

1.1.5 Esta DPC segue as atualizações dos documentos *Baseline Requirements* e *Extended Validation* SSL e *CodeSign Guidelines* [11], do *WebTrust Principles and Criteria* [10] e publicações do CA/*Browser Forum*, disponíveis no sítio https://cabforum.org.

1.1.6 A estrutura desta DPC está baseada na RFC 3647 [13].

1.2 Nome do documento e identificação

Esta DPC é chamada "DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL" e comumente referida como "DPC da AC Raiz". O *Object Identifier* – OID desta DPC é 2.16.76.1.1.0.

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora Raiz – AC Raiz da ICP-Brasil.

1.3.2 Autoridades de Registro

A atividade de identificação e cadastramento das ACs de nível imediatamente subsequente ao da AC Raiz será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro - AR no âmbito da AC Raiz.

1.3.3 Titulares do certificado

Os certificados emitidos pela AC Raiz têm como titulares a própria AC Raiz ou as ACs de nível imediatamente subsequente ao seu.

1.3.4 Partes confiáveis

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

1.3.5 Outros participantes

A Universidade Federal de Santa Catarina - UFSC é um participante prestando serviço de suporte à AC Raiz, disponibilizando infraestrutura física e lógica (ambiente de contingência) e recursos humanos especializados.

1.4 Usabilidade do certificado

1.4.1 Uso apropriado do certificado

Os certificados emitidos pela AC Raiz têm como objetivo único identificar a própria AC Raiz ou as ACs de nível imediatamente subsequente ao seu e divulgar suas chaves públicas de forma segura.

1.4.2 Uso proibitivo do certificado

Os certificados emitidos pela AC Raiz não podem identificar ou verificar qualquer entidade ou assinatura além dos propósitos descritos nesta DPC.

1.5 Política de Administração

1.5.1 Organização administrativa do documento

Nome: Instituto Nacional de Tecnologia da Informação - ITI

1.5.2 Contatos

Endereço: SCN, Quadra 2, Bloco E, CEP 70.712-905, Brasília-DF – Brasil

Telefone: (61) 3424-3853, 3424-3854, 3424-3856

Fax: (61) 3424-3910

Página web: http://www.iti.gov.br

E-mail: cgope@iti.gov.br

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Este documento consolida a DPC e PC da AC Raiz.

1.5.4 Procedimentos de aprovação da DPC

1.5.4.1 Esta DPC é aprovada pelo CG ICP-Brasil, por meio de análise e voto dos seus membros integrantes.

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

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridade de Registro
CG ICP-BRASIL	Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira
DN	*Distinguished Name*
DOU	Diário Oficial da União
DPC	Declaração de Práticas de Certificação
DPCT	Declaração de Práticas de Carimbo do Tempo
DPPSC	Declaração de Práticas de Prestador de Serviço de Confiança
EAT	Entidade de Auditoria do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITI	Instituto Nacional de Tecnologia da Informação
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
OID	*Object Identifier*
PC	Política de Certificado
PCT	Política de Carimbo do Tempo

PCN	Plano de Continuidade de Negócio
PS	Política de Segurança
PSC	Prestadores de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
UTC	*Coordinated Universal Time*

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

São disponibilizados no repositório da AC Raiz, logo após sua emissão, os certificados por ela emitidos e sua LCR.

2.1 Repositórios

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

2.2 Publicação de informações dos certificados

2.2.1 O certificado da AC Raiz, sua LCR e os certificados das ACs de nível imediatamente subsequente ao seu são publicados nas páginas Web da AC Raiz http://acraiz.icpbrasil.gov.br e https://acraiz.icpbrasil.gov.br, obedecendo às regras e aos critérios estabelecidos nesta DPC.

2.2.2 A lista das Autoridades Certificadoras que integram a ICP-Brasil também é encontrada na página Web da AC Raiz.

2.2.3 A disponibilidade das informações publicadas pela AC Raiz em sua página Web, tais como certificados, sua LCR, sua DPC, entre outras, é de 99,99% (noventa e nove inteiros e noventa e nove décimos por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.2.4 A AC Raiz inclui nos certificados emitidos a identificação da sua página web.

2.2.5 A AC Raiz comunicará, por escrito, qualquer alteração nesta DPC às ACs integrantes da ICP-Brasil bem como a todas as ACs com as quais possui acordos de certificação cruzada. Dessa notificação constarão as alterações efetuadas.

2.3 Tempo ou frequência de publicação

Certificados são publicados imediatamente após sua emissão. A frequência da emissão de LCR e sua publicação estão descritos nos itens 4.9.7, 4.9.8 e 4.10 desta DPC.

2.4 Controle de acesso aos repositórios

2.4.1 Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC Raiz.

2.4.2 São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação dessas informações a pessoal autorizado. Há permissão somente de leitura.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Raiz verifica a autenticidade da identidade e/ou atributos das entidades da ICP-Brasil antes da inclusão desses atributos em um certificado digital. As entidades estão proibidas de usar nomes em seus certificados que violem os diretos de propriedade intelectual de terceiros. A AC Raiz reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1 Atribuição de nomes

3.1.1 Tipos de nomes

As ACs de nível imediatamente subsequente ao da AC Raiz, portanto titulares de certificados, terão um nome que as identifiquem univocamente no âmbito da ICP-Brasil. Essa identificação dar-se-á pelo DNs (*Distinguished Names*) – padrão ITU-T X.501.

3.1.2 Necessidade dos nomes serem significativos

Todos os certificados emitidos pela AC Raiz devem incluir um identificador único que represente a AC de nível imediatamente subsequente para a qual o certificado foi emitido, conforme item 7.1.4.

3.1.3 Anonimato ou pseudônimo dos titulares do certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

Nomes distintos em certificados são interpretados usando os padrões ITU-T X.501 e a sintaxe ASN.1.

3.1.5 Unicidade de nomes

Identificadores "*Distinguished Name*" - DN devem ser únicos para cada AC de nível imediatamente subsequente ao da AC Raiz. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU-T X.509. A extensão "*Unique Identifiers*" não será admitida para diferenciar as ACs com nomes idênticos.

3.1.6 Procedimento para resolver disputa de nomes.

A AC Raiz reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das ACs de nível imediatamente subsequente ao seu. Durante o processo de autenticação, a AC que solicita o certificado deve provar o seu direito de uso de um nome específico (DN) em seu certificado, de acordo com a legislação em vigor.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

3.1.7.1 As entidades não podem solicitar certificados com qualquer conteúdo que viole os direitos de propriedade intelectual de terceiros.

3.1.7.2 Não compete à AC Raiz verificar o direito do solicitante de usar uma marca registrada.

3.1.7.3 A AC Raiz se reserva o direito de revogar qualquer certificado envolvido em uma disputa.

3.2 Validação inicial de identidade

A AC Raiz realiza a identificação do solicitante ou de serviços, incluindo os serviços de encadeamento da Autoridade Certificadora, utilizando quaisquer meios legais de comunicação ou investigação necessárias para identificar a pessoa jurídica ou física.

3.2.1 Método para comprovar a posse de chave privada

A AC Raiz verifica se a AC credenciada possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. A RFC 4210 [14], atualizada pela RFC 6712 [16], é utilizada para essa finalidade.

3.2.2 Autenticação da identificação da organização

3.2.2.1 A identificação de uma AC pela AC Raiz é executada por meio dos procedimentos descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

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

3.2.3 Autenticação da identidade de um indivíduo

Não se aplica.

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 interoperabilidade

Não se aplica.

3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 Identificação e autenticação para rotina de novas chaves

3.3.1.1 O processo de geração, pela AC Raiz, de um novo certificado para uma AC de nível imediatamente subsequente ao seu pode ser feito de forma simplificada, antes da expiração da validade do certificado vigente da AC.

3.3.1.2 Para isso, um representante legal da AC deve preencher e assinar, em papel ou digitalmente, o FORMULÁRIO DE REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO [7]. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.

3.3.2 Identificação e autenticação para novas chaves após a revogação

A solicitação de novo certificado de AC após a revogação ou expiração do certificado anterior deverá ser efetivada pelo preenchimento do FORMULÁRIO DE REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO [7]. Esse formulário deverá ser assinado por representante legalmente constituído da AC e entregue junto à AC Raiz. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.

3.4 Identificação e autenticação para solicitação de revogação

3.4.1 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.

3.4.2 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

A AC Raiz mantém suas próprias listas de indivíduos e entidades das quais não aceitará solicitações de certificado. Além disso, outras fontes externas, como listas negadas pelo governo ou listas de pessoas negadas reconhecidas internacionalmente que são aplicáveis às jurisdições em que a AC Raiz opera, são usadas para filtrar candidatos indesejados.

4.1.1 Quem pode submeter uma solicitação de certificado

4.1.1.1 A solicitação de um certificado da AC Raiz é feita pelo Comitê Gestor da ICP-Brasil que delega a execução dessas funções ao ITI.

4.1.1.2 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

Constituem responsabilidades da AC Raiz:

a) a geração e o gerenciamento do seu par de chaves criptográficas;

b) a emissão e distribuição do seu certificado digital;

c) a emissão, a expedição e a distribuição de certificados de AC de nível imediatamente subsequente ao seu;

d) a publicação de certificados por ela emitidos;

e) a revogação de certificados por ela emitidos;

f) a emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados – LCR;

g) a fiscalização e a auditoria das ACs, das Autoridades de Carimbo do Tempo - ACTs, das ARs, dos Prestadores de Serviço de Suporte -PSS, dos Prestadores de Serviço Biométrico - PSBio e dos Prestadores de Serviço de Confiança - PSC habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor da ICP-Brasil - CG da ICP-Brasil;

h) a implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil;

i) a adoção de medidas de segurança e controle, previstas nesta DPC e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [1], envolvendo seus processos, procedimentos e atividades;

j) a manutenção dos processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

k) a manutenção e garantia da integridade, do sigilo e da segurança da informação por ela tratada; e

l) a manutenção e o teste regular do seu Plano de Continuidade de Negócio - PCN.

4.2 Processamento de Solicitação de Certificado

4.2.1 Solicitação de certificado à AC Raiz

4.2.1.1 A solicitação de certificado para uma AC de nível imediatamente subsequente ao da AC Raiz só é possível após o deferimento de seu pedido de credenciamento e a consequente autorização de funcionamento da AC em questão por parte da AC Raiz, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.2.1.2 A AC de nível subsequente deve encaminhar a solicitação de seu certificado à AC Raiz 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.

4.2.1.3 A AC Raiz não recebe solicitações de certificados para usuários finais, de acordo com a MP nº 2.220-2, de 24 de agosto de 2001. Portanto, não existe, para a AC Raiz, o cenário de restrições ou autorizações ao processamento de registros de DNS para autorização da autoridade de certificação.

4.2.2 Execução das funções de identificação e autenticação

A AC Raiz executa as funções de identificação e autenticação conforme item 3.2 desta DPC.

4.2.3 Aprovação ou rejeição de pedidos de certificado

A AC raiz pode aceitar ou rejeitar pedidos de certificados das AC imediatamente subsequente de acordo com os procedimentos descritos no item 3.2 desta DPC.

4.2.4 Tempo para processar a solicitação de certificado

A AC Raiz garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 30 (trinta) dias úteis após a autorização de funcionamento da AC em questão.

4.3 Emissão de certificado

4.3.1 Ações da AC Raiz durante a emissão de um certificado

4.3.1.1 A emissão de um certificado pela AC Raiz é feita em cerimônia específica, com a presença de representante da AC Raiz, da AC credenciada, de auditores e convidados, na qual são registrados todos os procedimentos executados.

4.3.1.2 As chaves públicas dos certificados autoassinados são publicadas no DOU.

4.3.1.3 O certificado é considerado válido a partir do momento em que é emitido.

4.3.1.4 A emissão dos certificados da AC Raiz e das ACs de nível imediatamente subsequente é feita em equipamentos da AC Raiz que operam *off-line*.

4.3.1.5 A emissão de certificados pela AC Raiz para as ACs de nível imediatamente subsequente estará condicionada:

a) à apresentação de apólice de 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

b) ao pagamento da tarifa a que se refere o item 1.2 do documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [4].

4.3.1.6 A Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios está dispensada do pagamento da tarifa e da apresentação da apólice previstas no item anterior.

4.3.1.7 A AC Raiz entrega o certificado emitido, em formato definido conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil, para o representante legal da AC credenciada presente à cerimônia.

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

Após a emissão do certificado, a AC Raiz encaminha mensagem eletrônica de confirmação.

4.4 Aceitação de certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.1.1 Quando a AC Raiz emite um certificado para uma AC de nível imediatamente subsequente ao seu, ela garante que as informações contidas nesse certificado foram verificadas de acordo com esta DPC.

4.4.1.2 No momento da entrega do certificado, durante a cerimônia de sua emissão pela AC Raiz, a AC atesta o seu recebimento por meio de assinatura de Termo de Cerimônia de Emissão de Certificado, Termo de Cerimônia de Entrega de Chave Pública e Termo de Acordo por seu representante legal.

4.4.1.3 A aceitação do certificado se dá no momento em que os dados constantes do mesmo são verificados pela AC ou na primeira utilização da chave privada correspondente.

4.4.1.4 A verificação dos dados do certificado deve ser realizada pela AC titular no prazo de 2 (dois) dias úteis, contados a partir do seu recebimento, após o qual o certificado será considerado aceito.

4.4.1.5 Ao aceitar o certificado, a AC titular:

a) concorda com as responsabilidades, obrigações e deveres a ela impostas pelo Termo de Acordo e esta DPC;

b) garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado; e

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

4.4.1.6 A não aceitação de um certificado no prazo previsto implica a realização de nova cerimônia, onde é feita a revogação do certificado não aceito e a emissão de novo certificado.

4.4.2 Publicação do certificado pela AC Raiz

O certificado da AC Raiz 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 desta DPC.

4.5 Usabilidade do par de chaves e do certificado

A AC titular de certificado emitido pela AC Raiz deve 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 os documentos REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2] e REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3].

4.5.1 Usabilidade da chave privada e do certificado do titular

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

4.5.2 Usabilidade da chave pública e do certificado pelas terceiras partes confiáveis

4.5.2.1 As terceiras partes confiáveis devem estar em concordância com os termos estabelecidos nesta DPC, como condição de confiança no certificado.

4.5.2.2 Procedimentos para confiabilidade pela terceira parte confiável encontram-se descritos no item 9.6.4 desta DPC.

4.6 Renovação de certificados

Não se aplica.

4.6.1 Circunstâncias para renovação de certificados

Não se aplica.

4.6.2 Quem pode solicitar a renovação

Não se aplica.

4.6.3 Processamento de requisição para renovação de certificados

Não se aplica.

4.6.4 Notificação para nova emissão de certificado para o titular

Não se aplica.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Não se aplica.

4.6.6 Publicação de uma renovação de um certificado pela AC Raiz

Não se aplica.

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

Não se aplica.

4.7 Nova chave de certificado

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 Raiz

Não se aplica

4.7.7 Notificação de uma emissão de certificado pela AC Raiz 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 Raiz

Não se aplica

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

Não se aplica

4.9 Suspensão e revogação de certificado

4.9.1 Circunstâncias para revogação

4.9.1.1 Um certificado de AC de nível imediatamente subsequente ao da AC Raiz pode ser revogado a qualquer instante, por solicitação da própria AC titular do certificado ou por decisão motivada da AC Raiz, resguardados os princípios do contraditório e da ampla defesa.

4.9.1.2 Um certificado deve 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 da AC titular do certificado; ou

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

4.9.1.3 A AC Raiz pode revogar ou determinar a revogação do certificado ou da certificação cruzada, conforme o caso, 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 As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz.

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

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

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

4.9.2 Quem pode solicitar revogação

4.9.2.1 A revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Raiz somente pode ser feita:

a) por determinação da AC Raiz;

b) por solicitação da AC titular do certificado; ou

c) por determinação judicial.

4.9.3 Procedimento para solicitação de revogação

4.9.3.1 A solicitação de revogação do certificado à AC Raiz deve ser efetivada pelo preenchimento do FORMULÁRIO DE SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC [8]. Esse formulário deverá ser assinado por seu representante legal. Quando utilizada a versão eletrônica do formulário, ele deve ser assinado digitalmente e enviado à AC Raiz. O formulário pode também ser preenchido em papel, entregue pessoalmente pelo representante à AC Raiz e assinado no ato da entrega.

4.9.3.2 O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC Raiz da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC Raiz. Concluído esse processo, a AC Raiz informa à AC afetada a revogação do certificado.

4.9.3.3 O prazo para a revogação de certificado de AC de nível imediatamente subsequente ao da AC Raiz é de no máximo 24 (vinte e quatro) horas. O prazo contar-se-á a partir do recebimento pela AC Raiz da solicitação de revogação da AC titular do certificado ou da determinação de revogação emitida pela própria AC Raiz.

4.9.3.4 Um certificado de AC revogado somente pode ser usado para a verificação de assinaturas geradas durante o período em que o referido certificado esteve válido.

4.9.4 Prazo para solicitação de revogação

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

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

Conforme estabelecido no item 4.9.3.3.

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

O status dos certificados (para certificados revogados) estará disponível conforme item 2.1.

4.9.7 Frequência de emissão de LCR

4.9.7.1 A LCR da AC Raiz é atualizada, no máximo, a cada 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.9.3 e notifica todas as ACs de nível imediatamente subsequente ao seu.

4.9.7.2 Quando da revogação de certificado da própria AC Raiz, deverá ser emitida LCR com período de validade igual ao do certificado, encerrando a emissão de LCR por esta Autoridade Certificadora.

4.9.8 Latência máxima para a LCR

A LCR é divulgada no repositório dentro de um dia útil após sua geração.

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

Não serão aceitos pedidos de revogação *on-line* ao sistema de certificação da AC Raiz. A única forma de consulta *on-line* de status de certificado é a realizada por meio da LCR.

4.9.10 Requisitos para verificação de revogação *on-line*

Não se aplica.

4.9.11 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subsequente ao da AC Raiz e os autoassinados da AC Raiz também podem ser divulgadas por meio de sua publicação no Diário Oficial da União ou na página web da AC Raiz.

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.12.1 No caso do comprometimento da chave privada de uma AC de nível imediatamente subsequente ao da AC Raiz, a mesma deve notificar a AC Raiz.

4.9.12.2 Uma AC deve garantir que a sua DPC contenha determinações que definam os meios que serão utilizados para se notificar um comprometimento ou suspeita de comprometimento.

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 ao da AC Raiz.

4.9.14 Quem pode solicitar suspensão

AC Raiz ou AC subsequente, 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 Raiz fornece um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados.

4.10.2 Disponibilidade dos serviços

Ver item 2.2 desta DPC.

4.10.3 Funcionalidades operacionais

Ver item 4.9 desta DPC.

4.11 Encerramento de atividades

Observado o disposto no item "Descredenciamento" do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], a DPC da AC subsequente deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da AC responsável.

4.12 Custódia e recuperação de chave

Não é permitida a custódia (*escrow*) das chaves privadas da AC Raiz.

4.12.1 Política e práticas de custódia e recuperação de chave

Não se aplica à AC Raiz.

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

Não se aplica à AC Raiz.

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

O processo de gerenciamento de certificados da AC Raiz da ICP-Brasil inclui os seguintes controles:

a) segurança física e controles ambientais;

b) controles de integridade dos sistemas, incluindo gerenciamento de configuração, manutenção de integridade de código confiável e detecção e prevenção de incidentes;

c) segurança de rede e gerenciamento de *firewalls*, incluindo restrições de porta e filtragem de endereços IP;

d) gerenciamento de usuários, segregação de funções, capacitação, conscientização e treinamento;

e) controles de acesso lógico, com registro de atividades e de inatividade, a fim de fornecer responsabilidades individuais; e

f) programa de segurança da AC Raiz da ICP-Brasil.

5.1 Controles físicos

A AC Raiz da ICP-Brasil mantém políticas de segurança para os ativos e sistemas usados nos processos de gerenciamento de certificados. Essas políticas cobrem controles de acesso físico, proteção contra desastres naturais, segurança contra incêndios, falhas de suporte (como energia, telecomunicações, links de dados, entre outros), colapso de estrutura, inundação, proteção contra roubo, acessos indevidos e recuperação de desastres. Estes controles devem ser implementados para evitar perda, danos ou comprometimento de ativos, interrupção das atividades do negócio relacionadas aos processos de gerenciamento de certificados, roubo de informações e comprometimento das instalações de processamento de informações.

5.1.1 Construção e localização das instalações

A AC Raiz da ICP-Brasil, para a execução das atividades relacionadas aos processos de gerenciamento certificados, utiliza instalações homologadas pelo Comitê Gestor da ICP-Brasil. Essas instalações devem estar de acordo com as normas de classificação e métodos de ensaio de resistência a fogo e práticas para segurança física relativa ao armazenamento de dados.

5.1.2 Acesso físico

5.1.2.1 O acesso físico às dependências da AC Raiz onde são realizadas as atividades relacionadas aos processos de gerenciamento de certificados da AC Raiz é gerenciado e controlado internamente de acordo com os requisitos definidos na Política de Segurança da ICP-Brasil.

5.1.2.2 O controle de acesso é realizado por meio de chaves, senhas, cartões criptográficos, identificações biométricas e outros dispositivos de forma que apenas pessoas autorizadas participem das atividades pertinentes. Além disso, o acesso físico e todos os ambientes são monitorados por meio de Circuito Fechado de TV (CFTV), com gravação digital 24x7.

5.1.2.3 O sistema de certificação da AC Raiz está situado em ambientes seguros redundantes, tipo sala-cofre, localizados em instalações geograficamente segredadas. Segurança física e controles de acesso através de identificação biométrica restringem o acesso aos equipamentos e sistemas relativos aos processos de gerenciamento de certificados.

5.1.2.4 São definidos pelo menos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC Raiz, e mais 2 (dois) níveis relativos à proteção das chaves privadas:

5.1.2.4.1 O **primeiro nível** – ou nível 1 – a primeira barreira de acesso às instalações da AC Raiz. No nível 1, cada indivíduo deverá ser identificado e registrado no interior de área guarnecida por segurança armada ou outro profissional qualificado, quando as instalações da AC Raiz se localizarem em área de segurança. A partir desse nível, pessoas estranhas à operação da AC transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo relacionado ao gerenciamento de certificados da AC deverá ser executado nesse nível.

5.1.2.4.2 Excetuados os casos previstos em lei, o porte de armas não será admitido nas instalações da AC Raiz, 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.

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

5.1.2.4.4 O **terceiro nível** – ou nível 3 – situa-se dentro do segundo e será o primeiro nível a abrigar material e atividades sensíveis relacionados aos processos de gerenciamento de certificados da AC Raiz.

5.1.2.4.5 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.

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

5.1.2.4.7 Telefones celulares, bem como outros equipamentos portáteis de comunicação e armazenamento de dados, exceto aqueles exigidos para a operação da AC Raiz, não são admitidos a partir do nível 3.

5.1.2.4.8 **Quarto nível** – ou nível 4 – interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Raiz, tais como a emissão e revogação de certificados e a emissão de LCR. Todos os sistemas e equipamentos necessários a essas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas deverá ser exigida enquanto o ambiente estiver ocupado.

5.1.2.4.9 No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são 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 permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre – possuem proteção contra interferência eletromagnética externa ou possuem equipamentos, tipo rack, que possuem tal característica.

5.1.2.4.10 As salas-cofre são construídas segundo as normas brasileiras aplicáveis e eventuais omissões dessas normas são sanadas por normas internacionais pertinentes.

5.1.2.4.11 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).

5.1.2.4.12 As portas de acesso à sala-cofre constituem eclusas, onde uma porta só deverá se abrir quando a anterior estiver fechada.

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

5.1.2.4.14 **Quinto nível** – ou nível 5 – interior aos ambientes de nível 4, compreendem um cofre ou um gabinete reforçado trancado. Materiais criptográficos, tais como, chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

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

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

b) possuir tranca com chave.

5.1.2.4.16 **Sexto nível** – ou nível 6 – consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de acesso individual ao seu conteúdo. Os dados de ativação da chave privada da AC Raiz são armazenados nesses depósitos.

5.1.3 Sistemas físicos de detecção

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

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

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

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

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

5.1.3.6 O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por profissional qualificado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações dos profissionais de monitoramento.

5.1.4 Mecanismos de emergência

5.1.4.1 Mecanismos específicos são implantados pela AC Raiz para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos acionam imediatamente os alarmes de abertura de portas.

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

5.1.5 Energia e ar-condicionado

5.1.5.1 A infraestrutura do ambiente de certificação da AC Raiz é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC Raiz e seus respectivos serviços.

5.1.5.2 As instalações da AC Raiz, além de estarem conectadas à rede elétrica provida pela concessionária de energia, dispõem de recursos que garantem a capacidade de redundância de toda a estrutura de energia e ar-condicionado para sua operação ininterrupta, mesmo em caso de falha no fornecimento de energia pela concessionária. São eles:

a) gerador de energia de porte compatível;

b) gerador de energia em reserva, operando de forma redundante;

c) sistema para fornecimento de energia ininterrupta (*no-breaks*) redundante;

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

e) iluminação de emergência.

5.1.5.3 Todos os cabos elétricos estão protegidos por tubulações ou dutos apropriados. São utilizadas 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. São utilizados dutos separados para os cabos de energia, de telefonia e de dados. Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 (seis) meses, na busca de evidências de violação ou de outras anormalidades.

5.1.5.4 O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente, dispõe de filtros de poeira e é independente do sistema de ar-condicionado do edifício onde está localizado.

5.1.5.5 Nos ambientes de nível 4, o sistema de climatização é independente, tolerante a falhas, redundante e composto por sistemas de ar-condicionado de precisão e refrigeração de conforto para área administrativa e demais ambientes. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta e a temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.6 Exposição à água

A estrutura inteiriça do ambiente de nível 4 da AC Raiz é construída na forma de uma célula estanque, a fim de prover a proteção física contra infiltrações e inundações provenientes de qualquer fonte externa. Além disso, existe um sistema de alarme de detecção de umidade e uma equipe de monitoração pronta para responder a qualquer exposição improvável à água.

5.1.7 Prevenção e proteção contra incêndio

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

5.1.7.2 As instalações possuem sistema de detecção de fumaça, sistema de detecção precoce de incêndio, por meio da análise de partículas iônicas, e sistema de extinção de incêndio por gás inerte, não corrosivo, não combustível e não reagente com a maioria das substâncias.

5.1.7.3 Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam 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.

5.1.7.4 Em caso de incêndio nas instalações da AC Raiz, o aumento da temperatura interna dentro da sala-cofre não deverá exceder a 50 (cinquenta) graus Celsius e a sala deverá suportar essa condição por pelo menos 1 (uma) hora.

5.1.8 Armazenamento de mídia

A AC Raiz atende à norma brasileira NBR 11.515/NB 1334 - Critérios de Segurança Física Relativos ao Armazenamento de Dados [12] para garantir a segurança de mídias armazenadas, dispondo de ambientes específicos que garantem que as mídias neles armazenadas não sofram nenhum tipo de dano gerado por fatores externos e protegidos contra danos causados por fogo e água.

5.1.9 Destruição de lixo

Todos os documentos em papel com informações sensíveis são triturados antes de seu descarte. Todos os dispositivos eletrônicos não mais utilizáveis, que tenham sido utilizados anteriormente no armazenamento de informações sensíveis, são permanentemente apagados ou fisicamente destruídos.

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

A AC Raiz possui instalação de contingência (*off-site*) que atende aos mesmos requisitos de segurança da instalação principal. Sua localização é geograficamente separada da instalação principal de forma que, em caso de sinistro que torne inoperante a instalação principal, a instalação de contingência não será atingida e pode se tornar totalmente operacional, em condições idênticas em, no máximo, 48 (quarenta e oito) horas.

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

5.2.1.1 A AC Raiz garante a segregação das tarefas para funções críticas, com o intuito de evitar conflitos de interesse e prover a segurança adequada das operações. As ações de cada individuo estão limitadas de acordo com o perfil a que está associado.

5.2.1.2 A AC Raiz estabelece os seguintes perfis confiáveis distintos: coordenação da infraestrutura, coordenação da segurança, operação da AC Raiz, operação da entidade de auditoria de tempo – EAT, auditoria e detentores da chave de ativação das cadeias de certificação. A divisão de responsabilidades estão distribuídas como se seguem:

a) Coordenação da infraestrutura: Planejar, coordenar e acompanhar os processos referentes à gestão dos recursos de tecnologia de infraestrutura, especialmente os relacionados a *software*, sistemas de informação, bancos de dados e redes de comunicação; manter a disponibilidade da infraestrutura para a publicação das informações; coordenar e acompanhar as atividades de implantação e manutenção de sistemas de informação e criptográficos da AC Raiz e da EAT; realizar a instalação, customização e integração dos sistemas de informação adquiridos ou desenvolvidos no âmbito da AC Raiz; responsável pela gestão de mudanças e controle de configurações;

b) Coordenação da segurança: Planejar, coordenar e acompanhar a gestão de continuidade da AC Raiz, do repositório de Políticas de Assinatura, certificados e LCRs, bem como da EAT; coordenar e acompanhar as atividades referentes à política de acesso e gerenciamento do ambiente de TI, a fim de garantir a segurança; manter e garantir a integridade, o sigilo e a segurança da informação tratada pela AC Raiz; acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança; responsabilizar-se pela implementação das práticas e políticas de segurança e gerenciamento dos operadores da AC Raiz; identificar, mapear e analisar os riscos; elaborar planos de ação apropriados para os riscos identificados; e elaborar o plano de contingência de tecnologia para a infraestrutura da AC Raiz;

c) Operação da AC Raiz: Gerenciar a implantação, manutenção e operação dos sistemas criptográficos da AC Raiz da ICP-Brasil; gerenciar o ciclo de vida dos certificados; coordenar a emissão, publicação e revogação dos certificados no âmbito da AC Raiz da ICP-Brasil; gerenciar conteúdos dos repositórios da AC Raiz e coordenar os processos de gestão de pessoas envolvidas nas atividades da AC Raiz;

d) Operação da Entidade de Auditoria de Tempo: Coordenar e acompanhar as atividades da AC Raiz e da EAT quanto à definição, execução, desenvolvimento e aquisição de sistemas de carimbo do tempo; coordenar a auditoria e sincronismo de Sistemas de Carimbo do Tempo das ACTs; operar a Entidade de Auditoria do Tempo – EAT da ICP-Brasil; coordenar a emissão, distribuição e revogação dos certificados da EAT; e coordenar o cadastramento, alteração e descadastramento de Autoridades de Carimbo do Tempo – ACT;

e) Auditoria: Responsável por acompanhar e fiscalizar o cumprimento das atividades de certificação em consonância com as normas e orientações da AC Raiz, responsável pela verificação do cumprimento desta DPC e da Política de Segurança no âmbito da AC Raiz;

f) Detentores da chave de ativação das cadeias de certificação: Pessoas designadas, a fim de representar os órgãos a seguir, que detêm as chaves para ativação das cadeias de certificação, necessárias para a operação do módulo de segurança criptográfico (*hardware*) da AC Raiz:

g) Presidência do ITI;

h) Diretoria de Infraestrutura de Chaves Públicas do ITI;

i) Diretoria de Auditoria, Fiscalização e Normatização do ITI;

j) Gabinete de Segurança Institucional da Presidência da República; e

k) Diretoria de Tecnologia da Presidência da República.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 O acesso ao sistema de gerenciamento de certificados, utilizado para a geração e revogação de certificados e geração de LCR, é realizado por meio de controle multiusuário, com o uso de segredo dividido, por pessoas com perfis confiáveis.

5.2.2.2 As chaves privadas das cadeias de certificação da AC Raiz são armazenadas em *hardware* criptográfico, localizado no interior de ambiente seguro – sala-cofre. É estabelecida a exigência de controle múltiplo para a utilização das chaves privadas da AC Raiz, de forma que pelo menos 3 (três) detentores de partição de segredo, dos 05 (cinco) possíveis, são requeridos para a utilização das chaves privadas das cadeias de certificação.

5.2.2.3 Todas as tarefas executadas no ambiente onde estiverem localizados os equipamentos de certificação da AC Raiz requererem a presença de, no mínimo, 2 (dois) de seus colaboradores com perfis qualificados conforme definido na Matriz de Perfil de Acesso. As demais tarefas da AC poderão ser executadas por um único colaborador com perfil qualificado.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1 Para a designação de pessoas para uma função confiável, AC Raiz executa uma verificação de antecedentes. Cada função descrita no item 5.2.1 desta DPC é identificada e autenticada de forma a garantir que a pessoa esteja designada na função certa, que possa apoiar as atividades da AC Raiz.

5.2.3.2 Todos os colaboradores da AC Raiz tem sua identidade e perfis verificados antes de:

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

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

c) receber credenciais para executar suas atividades operacionais na AC Raiz; e

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

5.2.3.3 Os certificados, contas e senhas utilizados para identificação e autenticação dos colaboradores devem:

a) ser diretamente atribuídos a uma única pessoa;

b) não permitir compartilhamento; e

c) ser restritos às ações associadas ao perfil para o qual foram designados.

5.2.4 Funções que requerem separação de deveres

A AC Raiz impõe a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1. Não é permitido, em nenhum caso, atuar nas seguintes funções concomitantemente:

a) Coordenação da Infraestrutura e Operação da AC Raiz ou Entidade de Auditoria do Tempo;

b) Coordenação da Segurança e Operação da AC Raiz ou Entidade de Auditoria do Tempo;

c) Auditoria e Coordenação da Infraestrutura ou da Segurança;

d) Auditoria e Operação da AC Raiz ou Entidade de Auditoria do Tempo.

5.3 Controles de Pessoal

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.1.1 Todo o pessoal da AC Raiz em atividades diretamente relacionadas ao ciclo de vida de certificados, como os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é admitido conforme o estabelecido na Politica de Segurança da ICP-Brasil.

5.3.1.2 Todos os colaboradores da AC Raiz que exercem perfis confiáveis ou executam funções críticas têm registrado em contrato ou termo de responsabilidade:

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

b) o compromisso de não divulgar informações sigilosas a que têm acesso.

5.3.1.3 Antes do envolvimento de qualquer pessoa no processo de gerenciamento de certificados, seja como servidor requisitado ou empregado contratado, a AC Raiz verifica a identidade e a confiabilidade de tal pessoa.

5.3.1.4 A AC Raiz emprega um número suficiente de colaboradores que possuem conhecimento especializado, experiência e as qualificações necessárias para as atividades que desempenha.

5.3.1.5 O pessoal da AC Raiz atende aos requisitos por meio de conhecimento especializado, experiência e qualificações com treinamento e educação formais e experiência real.

5.3.1.6 O pessoal da AC Raiz, servidores e ou empregados contratados, possuem atribuições definidas de acordo com o nível de responsabilidades, levando em conta a sensibilidade da posição e com base nos deveres e níveis de acesso, triagem de antecedentes, treinamento e capacitação. O pessoal da AC Raiz que atua diretamente com o sistema de gerenciamento de certificados é formalmente nomeado para funções de confiança.

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1 Todo o pessoal da AC Raiz em funções de confiança deve estar livre de conflitos de interesses que possam prejudicar a imparcialidade das operações da AC. Não é nomeada para uma função de confiança qualquer pessoa que possua antecedentes que possam ser inadequados ao cargo.

5.3.2.2 Todas as pessoas que ocuparem funções de confiança devem ser selecionadas com base na lealdade, confiabilidade e integridade, e devem estar sujeitas a investigação de antecedentes.

5.3.2.3 Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é, anualmente, submetido a:

a) verificação de antecedentes criminais;

b) verificação de situação de crédito;

c) verificação de histórico de empregos anteriores;

d) comprovação de escolaridade e de residência; e

e) assinatura de termos de sigilo e de responsabilidade específicos.

5.3.2.4 O pessoal não tem acesso às funções de confiança até que as verificações necessárias sejam concluídas e os resultados analisados.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento suficiente para o domínio dos seguintes temas:

a) política e procedimentos de segurança da AC Raiz;

b) *softwares* de certificação em uso na AC Raiz;

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

d) atividades sob sua responsabilidade.

5.3.3.2 A AC Raiz mantém registros de tais treinamentos e assegura que o pessoal mantenha o nível de habilidades que lhes permitam desempenhar suas tarefas satisfatoriamente.

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.4.1 Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados manter-se-á atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC Raiz.

5.3.4.2 A AC Raiz fornece treinamento em segurança da informação e gerenciamento do ambiente seguro pelo menos uma vez por ano a todos os colaboradores diretamente relacionados aos processos de certificação. Treinamentos de reciclagem são realizados pela AC Raiz sempre que houver a necessidade.

5.3.5 Frequência e sequência de rodízio de cargos

Não está definida a frequência para o rodízio de cargos, porém a AC Raiz garante que qualquer alteração na equipe não afetará a eficácia operacional ou a sua segurança.

5.3.6 Sanções para ações não autorizadas

Na eventualidade de uma violação das políticas ou ação não autorizada, real ou suspeita, realizada por pessoa relacionada aos processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC Raiz suspende imediatamente o seu acesso e privilégios, até que seja finalizada a apuração, e toma as medidas administrativas e legais cabíveis, aplicando as devidas sansões, conforme o caso.

5.3.7 Requisitos para contratação de pessoal

O empregado contratado da AC Raiz deve seguir o que está estabelecido na POLITICA DE SEGURANÇA DA ICP-BRASIL [1] para o exercício de suas atividades, estando sujeitos aos mesmos processos, procedimentos, avaliação, controle de segurança e treinamento que os servidores da AC Raiz.

5.3.8 Documentação fornecida ao pessoal

A AC Raiz disponibiliza para todo o seu pessoal:

a) DPC da AC Raiz;

b) Política de Segurança da ICP-Brasil;

c) documentação operacional relativa a suas atividades; e

d) contratos, normas, políticas e demais informações que sejam relevantes para suas atividades.

5.4 Procedimentos de *Log* de Auditoria.

5.4.1 Tipos de eventos registrados

5.4.1.1 Registros de auditoria são gerados para todos os eventos relacionados à operação e segurança e aos demais serviços da AC Raiz. Sempre que possível, os registros de auditoria de segurança são gerados automaticamente, quando não for possível, um livro de registro, formulário de papel ou outro mecanismo físico deve ser usado. Todos os registros de auditoria de segurança, eletrônicos ou não, são mantidos e disponibilizados para as auditorias de conformidade.

5.4.1.2 A AC Raiz garante que todos os eventos relacionados aos processos de gerenciamento de certificados sejam registrados de maneira a permitir a rastreabilidade. Todas as ações executadas pelo pessoal da AC Raiz, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou.

5.4.1.3 A AC Raiz registra em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos nos arquivos de auditoria:

a) iniciação e desligamento do sistema de certificação;

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

c) mudanças na configuração da AC Raiz e/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 Raiz;

h) emissão e revogação de certificados;

i) geração de LCR;

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

k) operações falhas de escrita e leitura no diretório de certificados e das LCRs.

5.4.1.4 Todos os registros de auditoria, eletrônicos ou manuais, devem conter a data e a hora do evento e a identificação do usuário que o realizou. A AC Raiz também coleta e consolida, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração dos sistemas;

c) mudanças de pessoal;

d) relatórios de discrepância e comprometimento; e

e) registros de inutilização de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.5 A fim de facilitar o processo de auditoria, todos os registros relacionados à operação e demais serviços da AC Raiz são coletados e consolidados, eletrônica ou manualmente, num local único, conforme a Politica de Segurança da ICP-Brasil.

5.4.2 Frequência de auditoria de registros

5.4.2.1 A AC Raiz garante que seus registros de auditoria são analisados, dependendo da sua criticidade, semanalmente, mensalmente ou sempre que houver a utilização de seu sistema de certificação (*offline*), ou ainda, em caso de suspeita de comprometimento da segurança.

5.4.2.2 Todos os eventos significativos são descritos em relatório de auditoria. Tal análise envolve uma inspeção breve de todos os registros verificando se não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades observadas. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3 Período de retenção para registros de auditoria

A AC Raiz mantém em suas próprias instalações, principal e de *backup*, os seus registros de auditoria por pelo menos 7 (sete) anos, ou mais se exigido em lei. A AC Raiz disponibiliza esses registros de auditoria para o auditor qualificado mediante solicitação.

5.4.4 Proteção de registros de auditoria

5.4.4.1 O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

5.4.4.2 Os eventos são registrados de maneira que são protegidos contra exclusão ou destruição (exceto para transferência para mídia de longo prazo).

5.4.4.3 Os registros de eventos são protegidos para evitar alterações e detectar adulteração e para garantir que apenas indivíduos com acesso autorizado possam realizar operações, sem modificar a integridade, autenticidade e confidencialidade dos dados, se necessária.

5.4.5 Procedimentos para cópia de segurança (*Backup*) de registros de auditoria

5.4.5.1 Os registros de eventos e sumários de auditoria do sistema de gerenciamento de certificados, plataformas criptográficas e demais componentes da infraestrutura, utilizados pela AC Raiz, possuem cópias de segurança semanais, mensais e anuais, ou sempre que houver alguma utilização desses equipamentos quando em ambiente *offline*.

5.4.5.2 Os registros de auditoria são armazenados em um local seguro (sala-cofre ou cofre de segurança) à prova de incêndio, sob o controle de pessoas autorizadas em função de confiança, e em local diferente dos componentes que os originaram. As cópias de segurança dos registros de auditoria são protegidas no mesmo grau dos originais.

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

5.4.6.1 O sistema de coleta de dados de auditoria interno à AC Raiz é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.6.2 Os processos de auditoria começam na inicialização dos sistemas e terminam apenas no seu desligamento. O sistema de coleta de auditoria garante a integridade e a disponibilidade dos dados coletados, e, se necessário, protege a sua confidencialidade.

5.4.7 Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que o causou, no entanto, eventos que são considerados possíveis problemas de violação de segurança envolvendo o ciclo de vida de certificados ou a infraestrutura, estes serão escalados para a equipe de segurança, a fim de que sejam adotadas as medidas cabíveis para correção ou mitigação.

5.4.8 Avaliações de vulnerabilidade

5.4.8.1 Os eventos que representem possível vulnerabilidade, detectados na análise dos registros de auditoria, são analisados detalhadamente e, dependendo de sua gravidade, são registrados em separado. Como decorrência, ações corretivas são implementadas e registradas para fins de auditoria.

5.4.8.2 A AC Raiz também realiza avaliação regular de vulnerabilidades cobrindo os principais ativos relacionados à emissão, divulgação e gerenciamento de certificados.

5.5 Arquivamento de Registros

5.5.1 Tipos de registros arquivados

5.5.1.1 A AC Raiz armazena registros com os detalhes suficientes para estabelecer a validade de uma assinatura e da operação adequada do sistema da AC.

5.5.1.2 São armazenadas informações de auditoria detalhadas no item 5.4.1 e os processos de credenciamento de AC de nível imediatamente subsequente ao da AC Raiz.

5.5.2 Período de retenção para arquivo

A documentação relativa aos eventos relacionados no item anterior são retidos pelo seguinte período:

a) certificados de assinatura digital e respectivas LCR deverão ser retidos permanentemente, para fins de consulta histórica;

b) as cópias dos processos de credenciamento de AC por, no mínimo, 30 (trinta) anos a contar da data de expiração ou revogação do certificado; e

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

5.5.3 Proteção de arquivo

5.5.3.1 Todos os arquivos são protegidos e armazenados fisicamente com os mesmos requisitos de segurança que os de sua instalação. As cópias de segurança das informações são mantidas em um local distinto e separado dos que os originaram, com requisitos de segurança e disponibilidade.

5.5.3.2 Os arquivos são criados de tal forma que não podem ser excluídos ou destruídos (exceto após transferência para mídia de longo prazo) pelo período de tempo em que devem ser retidos. As proteções de arquivamento garantem que apenas o acesso confiável autorizado possa fazer operações, sem modificar a integridade, a autenticidade e a confidencialidade dos dados. Se a mídia original não puder reter os dados pelo período necessário, deverá ser definido um mecanismo para transferência periódica dos dados arquivados para novas mídias.

5.5.4 5.5.4 Procedimentos de cópia de arquivo

5.5.4.1 Uma segunda cópia de todo o material descrito no item 5.4.1 é armazenada em local externo à AC Raiz, recebendo o mesmo tipo de proteção utilizada por ela. Essas cópias seguem os períodos de retenção definidos para os registros dos quais são cópias de segurança. A AC Raiz deve verificar a integridade das cópias de segurança, pelo menos, a cada 6 (seis) meses.

5.5.4.2 São realizadas cópias de segurança para arquivamento dos sistemas da AC Raiz *on-line* ou do sistema *offline*. As cópias de segurança são armazenadas em um cofre de mídia classificado contra fogo. A cópia de segurança das informações do ambiente *offline* é realizada no final de qualquer cerimônia e armazenada em um local fora do ambiente, seguindo os mesmos critérios de segurança.

5.5.5 Requisitos para datação de registros

Informações de data e hora dos registros baseiam-se na hora oficial internacional, *Coordinated Universal Time* – UTC e obedecem ao formato YYYYMMDDHHMMSSZ, incluindo segundos mesmo que o número de segundos seja zero.

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

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Raiz em seus procedimentos operacionais são internos. O sistema de coleta de dados atende aos requisitos de segurança deste item 5.

5.5.7 Procedimentos para obter e verificar informação de arquivo

5.5.7.1 As mídias de armazenamento das informações são verificadas na criação. Periodicamente, amostras estatísticas de informações arquivadas são testadas para verificar a integridade e legibilidade contínuas das informações, por meio de procedimentos de restauração.

5.5.7.2 Somente equipamentos autorizados da AC Raiz, pessoas em funções confiáveis e outras pessoas autorizadas podem ter acesso aos arquivos. As solicitações para obtenção das informações são coordenadas por administradores do ambiente seguro em funções de confiança (Auditoria, Coordenação de Infraestrutura e Coordenação de Segurança).

5.5.7.3 A verificação de informação de arquivo deve ser solicitada formalmente à AC Raiz, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

5.6 Troca de chave

5.6.1 A AC de nível imediatamente subsequente ao da AC Raiz deverá iniciar, até 3 (três) meses antes da data de expiração do seu certificado, o processo de geração de novo par de chaves e de emissão de novo certificado.

5.6.2 Revogado ou expirado o certificado de uma AC de nível imediatamente subsequente ao seu, a AC Raiz remove imediatamente esse certificado do diretório e de sua página web, mantendo-o armazenado permanentemente para efeito de consulta histórica.

5.6.3 As chaves privadas usadas para assinar os certificados das ACs subsequentes devem ser mantidas até o momento em que todos os certificados das ACs tenham expirado.

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Procedimentos de gerenciamento de incidente e comprometimento

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

5.7.1.2 A AC Raiz testa, revisa e atualiza anualmente esses procedimentos. O Plano de Continuidade de Negócios deve incluir, no mínimo:

a) as condições para ativar o plano;

b) procedimentos de emergência;

c) procedimentos de *fallback*;

d) procedimentos de restauração;

e) cronograma para manutenção do plano;

f) requisitos de conscientização e educação;

g) responsabilidades individuais;

h) Objetivo de Tempo de Recuperação (RTO);

i) testes regulares dos planos de contingência;

j) o plano para manter ou restaurar as operações de negócios da AC Raiz de forma oportuna, após a interrupção ou falha de processos críticos de negócios;

k) definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;

l) definição de interrupções aceitáveis do sistema e um tempo de recuperação;

m) frequência para realização de cópias de *backup*;

n) distância entre as instalações de recuperação e o site principal da AC Raiz; e

o) procedimentos para proteger suas instalações após um desastre e antes de restaurar o ambiente seguro no local original ou remoto.

5.7.2 Recursos computacionais, software e/ou dados corrompidos

5.7.2.1 A AC Raiz mantém um site de contingência em um local geograficamente separado que espelha sua instalação principal para que, se algum *software* ou dados forem corrompidos, possa ser restaurado a partir do site de *backup* por meio de uma conexão segura. As cópias de segurança de todos os *softwares* e dados relevantes são obtidos regularmente em ambos os sites.

5.7.2.2 Se algum equipamento for danificado ou tornado inoperante, mas as chaves privadas não forem destruídas, a operação deve ser restabelecida o mais rápido possível, dando prioridade à capacidade de gerar informações de status de certificado – LCRs, de acordo com o Plano de Recuperação de Desastres da AC Raiz. Demais procedimentos estão descritos no PCN da AC Raiz.

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 No caso de uma chave privada da AC Raiz ou ACs subsequentes ser comprometida, perdida ou destruída:

a) todos os usuários que receberam um certificado deverão ser notificados o mais rapidamente possível; e

b) um novo par de chaves da AC deve ser gerado ou uma hierarquia alternativa de AC existente deve ser usada para gerar novos certificados.

5.7.3.2 Demais procedimentos estão descritos no PCN da AC Raiz.

5.7.4 Capacidade de continuidade de negócio após desastre

5.7.4.1 A equipe de infraestrutura e segurança usará todos os meios razoáveis para monitorar a instalação da AC Raiz após um desastre natural ou outro tipo de desastre, a fim de proteger contra perdas, danos adicionais e roubo de materiais e informações confidenciais.

5.7.4.2 O Plano de Recuperação de Desastres junto com o Plano de Continuidade dos Negócios, conforme descrito no item 5.7.1, estabelece procedimentos para que as informações sobre o status de certificados estejam disponíveis 24 horas por dia, 365 dias por ano.

5.8 Extinção da AC Raiz

No caso da necessidade de encerrar a operação da AC Raiz, o impacto da rescisão deve ser minimizado o máximo possível, levando em conta a prevalência de circunstâncias. Neste caso, deverão ser tomadas, no mínimo, as seguintes providências:

a) realizar a notificação de todas as entidades integrantes da ICP-Brasil;

b) garantir que qualquer interrupção causada pelo término da AC Raiz seja minimizada o máximo possível;

c) garantir que os registros arquivados da AC Raiz sejam mantidos;

d) garantir que os serviços de informações de estado de certificados sejam fornecidos e mantidos pelo período aplicável;

e) manter a operação da AC Raiz pelo período mínimo de 1 (um) ano após a notificação de sua extinção, salvo em casos de sucessão;

f) ajudar com a transferência ordenada de serviços e registros operacionais para um sucessor da AC Raiz, se houver;

g) garantir que seja mantido um processo de revogação de todos os certificados digitais emitidos pela AC Raiz; e

h) armazenar os dados da AC Raiz pelo período previsto na legislação.

5.9 Programa de segurança da AC Raiz

5.9.1 O programa de segurança da AC Raiz da ICP-Brasil inclui uma Avaliação de Risco anual que:

a) identifica ameaças internas e externas previsíveis que podem resultar em acesso não autorizado, divulgação, uso indevido, alteração ou destruição de quaisquer dados de certificados ou processos de gerenciamento de certificados;

a) avalia a probabilidade e possíveis danos causados por essas ameaças, levando em consideração a sensibilidade dos dados de certificado e os processos de gerenciamento de certificados; e

b) avalia a suficiência das políticas, procedimentos, sistemas de informação, tecnologia e outras providências que a ICP-Brasil tem em vigor para combater tais ameaças.

5.9.2 Com base na Avaliação de Riscos, a AC Raiz da ICP-Brasil desenvolve, implementa e mantém um Plano de Segurança que consiste em procedimentos, medidas e produtos de segurança projetados para alcançar os objetivos estabelecidos acima e para gerenciar e controlar os riscos identificados durante o processo de Avaliação de Riscos.

5.9.3 O Plano de Segurança inclui salvaguardas administrativas, organizacionais, técnicas e físicas apropriadas à sensibilidade dos dados de certificado e do processo de gerenciamento de certificados. O Plano de Segurança também leva em conta a tecnologia disponível e o custo de implementação das medidas de controle e implementa um nível aceitável de segurança apropriado aos danos que podem resultar de uma violação de segurança e da criticidade dos dados a serem protegidos.

6 CONTROLES TÉCNICOS DE SEGURANÇA

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, regulamento editado por instrução normativa da AC Raiz .

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1 O par de chaves criptográficas da AC Raiz é gerado pela própria AC Raiz, em *hardware* específico, conforme regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.2 O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC Raiz é gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.3 Os algoritmos e dispositivos criptográficos a serem utilizados para as chaves criptográficas da AC Raiz estão definidos em regulamento editado por instrução normativa da AC Raiz..

6.1.2 Entrega da chave privada à entidade

Não se aplica.

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1 A AC de nível imediatamente subsequente ao da AC Raiz entrega à AC Raiz cópia de sua chave pública, em formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.3.2 Essa entrega é feita por representante legalmente constituído da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4 Entrega de chave pública da AC Raiz às terceiras partes

6.1.4.1 A entrega do certificado da AC Raiz para as ACs de nível imediatamente subsequente ao seu é feita no momento da disponibilização do certificado da AC, utilizando-se para isto o formato definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.4.2 A disponibilização do certificado da AC Raiz para os demais usuários e partes da ICP-Brasil é realizada por uma das seguintes formas:

a) no momento da disponibilização do certificado para seu titular;

b) em diretório;

c) na página web da AC Raiz ou das ACs e ACT integrantes da ICP-Brasil; ou

d) por outros meios seguros definidos pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

O tamanho das chaves criptográficas assimétricas da AC Raiz e das ACs de nível imediatamente subsequente ao seu encontra-se definido 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 Os parâmetros de geração de chaves assimétricas da AC Raiz adotam 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 são verificados de acordo com as normas referenciadas 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)

A chave privada da AC Raiz é utilizada apenas para a assinatura de seu próprio certificado, dos certificados das ACs de nível imediatamente subsequente ao seu e de sua LCR.

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

A chave privada da AC Raiz é armazenada de forma cifrada no mesmo componente seguro de *hardware* utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

6.2.1 Padrões e controle para módulo criptográfico

O módulo criptográfico da AC Raiz adota o padrão definido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.2.2 Controle “n de m” para chave privada

A chave criptográfica de ativação do componente seguro de *hardware* que armazena a chave privada da AC Raiz é dividida em 5 (cinco) partes e distribuída entre 5 (cinco) pessoas designadas pela AC Raiz. É necessária a presença de apenas 3 (três) dessas 5 (cinco) pessoas para a ativação do componente e a consequente utilização da chave privada da AC Raiz.

6.2.3 Custódia (*escrow*) de chave privada

Não é permitida a custódia (*escrow*) das chaves privadas da AC Raiz.

6.2.4 Cópia de segurança de chave privada

6.2.4.1 A AC Raiz mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.2 A AC Raiz não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subsequente ao seu.

6.2.5 Arquivamento de chave privada

Não se aplica.

6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da AC Raiz é inserida no módulo criptográfico de acordo com o estabelecido nos Manuais de Conduta Técnica da ICP-Brasil.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.1.

6.2.8 Método de ativação de chave privada

A ativação da chave privada da AC Raiz é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de dispositivo de controle de acesso em *hardware* (*token*).

6.2.9 Método de desativação de chave privada

Quando a chave privada da AC Raiz for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco onde a chave eventualmente estivesse armazenada deve ser sobrescrito.

6.2.10 Método de destruição de chave privada

Além do estabelecido no item 6.2.9, todas as cópias de segurança da chave privada da AC Raiz devem ser destruídas, como também todos os discos rígidos, *tokens*, módulos criptográficos e qualquer mídia de armazenamento que as tenham hospedado por algum período.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas da AC Raiz e das ACs de nível imediatamente subsequente ao seu são armazenadas permanentemente, após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

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

A chave privada da AC Raiz é utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC Raiz pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Os dados de ativação da chave privada da AC Raiz são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em *hardware* (*token*).

6.4.2 Proteção dos dados de ativação

Os dados de ativação da chave privada da AC Raiz são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.3 Outros aspectos dos dados de ativação

Não se aplica.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1 A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subsequente ao seu deve ser realizada num ambiente *off-line*, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente *off-line*, com acesso restrito.

6.5.1.2 Cada computador servidor da AC Raiz diretamente relacionado com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados possui as seguintes características:

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

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

c) uso de criptografia para segurança de base de dados;

d) geração e armazenamento de registros de auditoria da AC Raiz;

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

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

6.5.2 Classificação da segurança computacional

Não se aplica.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistema

A AC Raiz utiliza um *software* projetado e desenvolvido por meio de uma metodologia formal rigorosa, específica para ambientes de segurança crítica.

6.6.2 Controles de gerenciamento de segurança

Uma metodologia formal de gerenciamento de configuração é usada para instalação e contínua manutenção do sistema de certificação da AC Raiz. Novas versões desse *software* somente são instaladas após comunicação do fabricante e testes em ambiente de homologação da AC Raiz.

6.6.3 Controles de segurança de ciclo de vida

Não se aplica.

6.7 Controles de Segurança de Rede

O computador servidor da AC Raiz que hospeda o sistema de certificação opera *off-line*, fisicamente desconectado de qualquer rede.

6.8 Carimbo de Tempo

Não se aplica.

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil de Certificado

O formato de todos os certificados emitidos pela AC Raiz está em conformidade com o padrão ITU-T X.509 ou ISO/IEC 9594, observando:

a) o certificado da AC Raiz é o único certificado autoassinado da ICP-Brasil, com validade máxima de 20 (vinte) anos quando da utilização de criptografia de curvas elípticas, ou 13 (treze) anos para os demais casos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

b) o certificado da AC de nível subsequente ao da AC Raiz é assinado pela AC Raiz e possui validade limitada à validade do certificado da AC Raiz, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

7.1.1 Número de versão

7.1.1.1 O certificado da AC Raiz implementa a versão 3 de certificado do padrão ITU-T X.509.

7.1.1.2 O certificado da AC de nível imediatamente subsequente ao da AC Raiz implementa a versão 3 de certificado do padrão ITU-T X.509.

7.1.2 Extensões de certificado

7.1.2.1 O certificado da AC Raiz implementa as seguintes extensões previstas na versão 3 do padrão ITU-T X.509:

a) ***basicConstraints***: contém o campo cA=True. O campo *pathLenConstraint* não é utilizado.

b) ***keyUsage***: contém apenas os bits *keyCertSign*(5) e *cRLSign*(6) ligados. Os demais bits estão desligados.

c) ***cRLDistributionPoints***: contém o endereço na Web onde se obtém a LCR correspondente ao certificado:

i. para certificados da cadeia inicial: http://acraiz.icpbrasil.gov.br/LCRacraiz.crl;

ii. para certificados da cadeia V1: http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl;

iii. para certificados da cadeia V2: http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl;

iv. para certificados da cadeia V3: http://acraiz.icpbrasil.gov.br/LCRacraizv3.crl;

v. para certificados da cadeia V4: http://acraiz.icpbrasil.gov.br/LCRacraizv4.crl.

vi. para certificados da cadeia V5: http://acraiz.icpbrasil.gov.br/LCRacraizv5.crl.

vii. para certificados da cadeia V6: http://acraiz.icpbrasil.gov.br/LCRacraizv6.crl.

viii. para certificados da cadeia V7: http://acraiz.icpbrasil.gov.br/LCRacraizv7.crl.

ix. para certificados da cadeia V8: http://acraiz.icpbrasil.gov.br/LCRacraizv8.crl.

x. para certificados da cadeia V9: http://acraiz.icpbrasil.gov.br/LCRacraizv9.crl.

xi. para certificados da cadeia V10: http://acraiz.icpbrasil.gov.br/LCRacraizv10.crl.

xii. para certificados da cadeia V11: http://acraiz.icpbrasil.gov.br/LCRacraizv11.crl.

d) ***Certificate Policies***: especifica o *Object Identifier* (OID) da DPC da AC Raiz e o atributo id-qt-cps com o endereço na Web desta DPC L(http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf).

e) ***SubjectKeyIdentifier***: contém o *hash* da chave pública da AC Raiz.

7.1.2.2 O certificado da AC de nível imediatamente subsequente ao da AC Raiz pode implementar quaisquer das extensões previstas na versão 3 do padrão ITU-T X.509.

7.1.2.2.1 As seguintes extensões são obrigatórias:

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

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

c) **"*Key Usage*", crítica**: os bits *keyCertSign* e *cRLSign* devem estar ativados, podendo ser ativados outros *bits* para casos específicos;

d) **"*Certificate Policies*", não crítica**. O campo *policyIdentifier* deve conter:

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

ii. se a AC emite certificados para usuários finais, os OID das PCs implementadas, contendo o campo *policyQualifiers* com o atributo id-qt-cps e o endereço Web da DPC da AC.

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

f) **"*CRL Distribution Points*", não crítica**: deve conter endereço na Web onde se obtém a LCR correspondente ao certificado, conforme item 7.1.2.1.c.

7.1.2.2.2 Para ACs que emitem certificado SSL também são obrigatórias as extensões:

a) **"*Extended Key Usage*", não crítica**: deve conter o propósito *server authentication* OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito *client authentication* OID = 1.3.6.1.5.5.7.3.2; e

b) **"*Authority Information Access*", não crítica**: a primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação.

7.1.3 Identificadores de algoritmo

7.1.3.1 O certificado da AC Raiz é assinado 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.

7.1.3.2 O certificado de AC de nível subsequente ao da AC Raiz é assinado com o uso de 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 Os nomes do titular e do emissor do certificado da AC Raiz, constantes do campo "*Distinguished Name*" (DN), são os mesmos e seguem o padrão ITU-T X.501/ISO/IEC 9594-2, como abaixo descrito:

a) para certificado da cadeia inicial:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação - ITI

CN = Autoridade Certificadora Raiz Brasileira

b) para certificado da cadeia V1:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação - ITI

CN = Autoridade Certificadora Raiz Brasileira v1

c) para certificado da cadeia V2

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v2

d) para certificado da cadeia V3:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v3

e) para certificado da cadeia V4:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v4

f) para certificado da cadeia V5:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v5

g) para certificado da cadeia V6:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v6

h) para certificado da cadeia V7:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v7

i) para certificado da cadeia V8:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v8

j) para certificado da cadeia V9:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v9

k) para certificado da cadeia V10:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v10

l) para certificado da cadeia V11:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação – ITI

CN = Autoridade Certificadora Raiz Brasileira v11

7.1.4.2 Os nomes do titular e do emissor do certificado de AC de nível imediatamente subsequente ao da AC Raiz, constantes do campo "*Distinguished Name*" (DN), seguem o padrão ITU-T X.501/ISO/IEC 9594-2, da seguinte forma:

a) DN do titular:

C = BR

O = ICP-Brasil

OU = <CN da cadeia>

CN = <nome da AC subordinada>

b) DN do emissor:

C = BR

O = ICP-Brasil

OU = Instituto Nacional de Tecnologia da Informação - ITI

CN = <CN da cadeia>

7.1.5 Restrições de nome

7.1.5.1 Não são admitidos caracteres especiais ou de acentuação nos campos do DN.

7.1.5.2 O nome da AC titular do certificado deve ser submetido à aprovação no processo de credenciamento.

7.1.6 OID (Object Identifier) da DPC

O OID desta DPC é 2.16.76.1.1.0

7.1.7 Uso da extensão "*Policy Constraints*"

Não se aplica para AC Raiz. Se a AC emite certificados para usuários finais a extensão "*Policy Constraints*" poderá ser utilizada na forma definida pela RFC 5280 [15].

7.1.8 Sintaxe e semântica dos qualificadores de política

Os certificados emitidos pela AC Raiz implementam qualificadores de políticas na extensão "*Certificate Policies*", conforme descrito no item 7.1.2 desta DPC.

7.1.9 Semântica de processamento para as extensões críticas de PC

Não se aplica.

7.2 Perfil de LCR

Todos os certificados das ACs de nível imediatamente subsequente ao da AC Raiz devem ter a validade verificada na LCR da AC Raiz antes de serem utilizados. Também deve ser verificada a autenticidade da LCR da AC Raiz por meio da verificação da assinatura da AC Raiz e do período de validade da LCR.

7.2.1 Número(s) de versão

A AC Raiz implementa a sua LCR conforme a versão 2 do padrão ITU X.509.

7.2.2 Extensões de LCR e de suas entradas

A LCR emitida pela AC Raiz implementa as seguintes extensões previstas na RFC 5280 [15]:

a) ***AuthorityKeyIdentifier*:** contém o mesmo valor do campo "*Subject Key Identifier*" do certificado da AC Raiz;

b) ***cRLNumber***: contém um número sequencial para cada LCR emitida.

7.3 Perfil de OCSP

Não se aplica

7.3.1 Número(s) de versão

Não se aplica

7.3.2 Extensões de OCSP

Não se aplica

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

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 DPC, PCs, DPCT, PCTs, DPPSC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

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

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 [5].

8.3 Relação do avaliador com a entidade avaliada

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 [9].

8.4 Tópicos cobertos pela avaliação

Documentos Principais da ICP-Brasil (DOC-ICP-NN) e seus documentos suplementares (DOC-ICP-NN.nn), bem como as regulamentações aplicáveis para Auditoria WebTrust.

8.5 Ações tomadas como resultado de uma deficiência

CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [9] e CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

8.6 Comunicação dos resultados

CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [9] e CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

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 [4].

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 gerenciada pela AC Raiz.

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 [4].

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura do seguro

Não se aplica.

9.2.2 Outros ativos

Não se aplica.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Não se aplica.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

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

9.3.2 Informações fora do escopo de informações confidenciais

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

9.3.2.2 Os seguintes documentos da AC Raiz, das ACs de nível imediatamente subsequente ao seu, das ACTs e PSCs também são considerados documentos não confidenciais:

a) qualquer PC aplicável;

b) qualquer DPC;

c) qualquer PCT aplicável;

d) qualquer DPCT;

e) qualquer DPPSC;

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

g) a conclusão dos relatórios da auditoria.

9.3.2.3 A AC Raiz 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

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.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC Raiz 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 Raiz 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 AC de nível imediatamente subsequente ao da AC Raiz são fornecidas na LCR da AC Raiz.

9.4.4 Responsabilidade para proteger a informação privadas

A AC Raiz é responsável pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas

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

9.4.5.2 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.

9.4.5.3 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

9.4.6.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC Raiz 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.

9.4.6.2 As informações privadas ou confidenciais sob a guarda da AC Raiz 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.

9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC Raiz

A AC Raiz declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

A AC Raiz e AC subsequentes implementam procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas, para AC Raiz, nos itens 3 e 4 desta DPC e ACs subsequentes nos documentos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3] e REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2]. A AC Raiz, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das ACs subsequentes na forma de suas DPCs, PCs e normas complementares.

9.6.1.2 Precisão da informação

A AC Raiz e AC subsequentes implementam procedimentos para verificar a precisão da informação contida nos certificados, contidas, para AC Raiz, nos itens 3 e 4 desta DPC e ACs subsequentes nos documentos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3] e REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2]. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes na forma de suas DPCs, PCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC Raiz e AC subsequentes implementam procedimentos para verificar identificação dos requerentes contida nos certificados, contidas, para AC Raiz, nos itens 3 e 4 desta DPC e ACs subsequentes nos documentos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3] e REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2]. A AC Raiz, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das ACs subsequentes na forma de suas DPCs, PCs e normas complementares.

9.6.1.4 Consentimento dos titulares

A AC Raiz e AC subsequentes implementam termos de consentimento ou titularidade, contidas, para AC Raiz, nos itens 3 e 4 desta DPC e ACs subsequentes em nos documentos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [3] e REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [2].

9.6.1.5 Serviço

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

9.6.1.6 Revogação

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

9.6.1.7 Existência Legal

Esta DPC está em conformidade legal com a MP nº 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

9.6.2 Declarações e Garantias da AR

Não se aplica.

9.6.3 Declarações e garantias do titular

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

9.6.3.2 A AC titular 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; e

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

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

a) tiver sido emitido pela AC Raiz;

b) não constar da última LCR da AC Raiz;

c) não estiver expirado; e

d) puder ser verificado com o uso do certificado válido da AC Raiz.

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 Raiz 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 Raiz 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

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

9.10.1 Término

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

9.10.2 Efeito da rescisão e sobrevivência

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

9.10.2.2 No caso de descredenciamento de AC subsequente à AC Raiz, os seguintes procedimentos devem ser adotados:

a) a AC Raiz divulgará o fato no Diário Oficial da União e em sua página web (repositório);

b) as ACs subsequentes, ARs e PSSs operacionalmente vinculados deverão cessar, em relação às PCs objeto do descredenciamento, suas atividades de emissão de certificados no âmbito da ICP-Brasil imediatamente após a comunicação de que trata a alínea anterior;

c) em caso de descredenciamento total de uma AC:

i. as chaves públicas dos certificados por ela emitidos deverão ser armazenadas por outra AC, após aprovação da AC Raiz;

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

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

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

9.10.2.3 No caso da AC Raiz, o Comitê Gestor da ICP-Brasil definirá os procedimentos de extinção.

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 pela AC Raiz à aprovação do CG da ICP-Brasil.

9.12.2 Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no DOU e no *site* do ITI.

9.12.3 Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13 Solução de conflitos

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

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 Raiz 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 Raiz. Havendo conflito entre esta DPC e outras resoluções do CG 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 alterado, 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
[1]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001	DOC-ICP-02
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL Aprovado pela Resolução nº 08, de 12 de dezembro de 2001	DOC-ICP-05
[3]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001	DOC-ICP-04
[4]	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
[5]	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
[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
[9]	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

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
[7]	FORMULÁRIO DE REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO	ADE-ICP.01.A
[8]	FORMULÁRIO DE SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC	ADE-ICP.01.B

10.3 Os documentos referenciados no *WebTrust Principles and Criteria* [10], bem como os *Baseline Requirements* e *Extended Validation* SSL e *CodeSign Guidelines* [11], são publicados respectivamente pelo CPA - *Chartered Professional Accountants* Canadá e CA/*Browser Forum*.

REF.	NOME DO DOCUMENTO	ENDEREÇO
[10]	WEBTRUST PRINCIPLES AND CRITERIA	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
[11]	BASELINE REQUIREMENTS, EXTENDED VALIDATION SSL e CODESIGN GUIDELINES	https://cabforum.org

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

[13] RFC 3647, IETF - *Internet* X.509 P*ublic Key Infrastructure Certificate Policy and Certification Practices Framework, november* 2003.

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

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

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