

ALTERADA EM 22.11.2001 PELA RESOLUÇÃO 04.
ALTERADA EM 14.02.2002 PELA RESOLUÇÃO 11.
ALTERADA EM 26.04.2002 PELA RESOLUÇÃO 13.
ALTERADA EM 29.08.2003 PELA RESOLUÇÃO 21.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 34.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 37.
REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 38

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 1, DE 25 DE SETEMBRO DE 2001.

Aprova a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.

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

RESOLVE:

Art. 1º Fica aprovada a DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AC RAIZ DA ICP-BRASIL em anexo.

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

MURILO MARQUES BARBOSA

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AC RAIZ DA ICP-BRASIL

1. INTRODUÇÃO

1.1. Visão Geral

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora Raiz (AC Raiz) da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços.

A AC Raiz possui o certificado de nível mais alto na ICP-Brasil. Este certificado contém a chave pública correspondente à chave privada da AC Raiz, utilizada para assinar o seu próprio certificado, os certificados das AC de nível imediatamente subsequente ao seu e sua LCR (Lista de Certificados Revogados).

Para requisitos relacionados a tipos específicos de certificado, a ICP-Brasil publica o documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil que serve como base para a elaboração das Políticas de Certificado (PC), sujeitas a esta DPC, que especificam como um tipo específico de certificado é gerado e administrado por uma AC, e utilizado pela comunidade.

A estrutura desta DPC está baseada na RFC 2527¹ (*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*).

1.2. Identificação

Esta DPC é chamada "Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil", e comumente referida como "DPC da AC Raiz".

1.3. Comunidade e Aplicabilidade

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 AC de nível imediatamente subsequente ao da AC Raiz será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro no âmbito da AC Raiz da ICP-Brasil.

1.3.3. Titulares de Certificado

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

1.3.4. Aplicabilidade

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

1.4. Dados de Contato (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

Nome: Instituto Nacional de Tecnologia da Informação -ITI

Endereço: Palácio do Planalto, Anexo IV

Telefone: (550xx61) 4112080, 411 3204, 4112781

Fax: 2265636

Página Web: <http://www.iti.gov.br>

E-mail: acraiz@iti.gov.br

2. DISPOSIÇÕES GERAIS

¹ RFC (Request for Comments), Internet Engineering task Force

2.1. Obrigações

2.1.1. Obrigações da AC Raiz

Constituem obrigações da AC Raiz da ICP-Brasil:

- A geração e o gerenciamento do par de chaves criptográficas da AC Raiz;
- A emissão e distribuição do certificado da AC Raiz;
- A emissão, a expedição e a distribuição de certificados de AC de nível imediatamente subsequente ao seu;
- A publicação de certificados por ela emitidos;
- A revogação de certificados por ela emitidos;
- A emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados (LCR);
- A fiscalização e a auditoria das AC, das AR e dos prestadores de serviço habilitados em conformidade com os critérios estabelecidos pelo CG da ICP-Brasil;
- A implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil;
- Adotar medidas de segurança e controle, previstas nesta DPC e na Política de Segurança da ICP-Brasil, envolvendo seus processos, procedimentos e atividades;
- Manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada; e
- Manter e testar regularmente planos de continuidade de negócio e de recuperação de desastres.

2.1.2. Obrigações da AR

Não se aplica.

2.1.3. Obrigações do Titular do Certificado

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.

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 Requisitos para DPC de AC e os Requisitos Mínimos para Políticas de Certificado na ICP-Brasil da ICP-Brasil.

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

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

2.1.4. Direitos da terceira parte (Relying Party)

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

Constituem direitos da terceira parte:

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

- verificar, a qualquer tempo, a validade do certificado. O certificado da AC Raiz ou um certificado de AC de nível imediatamente subsequente ao da AC Raiz é considerado válido quando:
- tiver sido emitido pela AC Raiz;
- não constar da LCR da AC Raiz;
- não estiver expirado; e
- puder ser verificado com o uso do certificado válido da AC Raiz.

2.1.5. Obrigações do Repositório

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

2.2. Responsabilidades

2.2.1. Responsabilidades da AC Raiz (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

A AC Raiz responde pelos danos a que der causa

2.2.2 Responsabilidades da AR

Não se aplica.

2.3. Responsabilidade Financeira

2.3.1. Indenizações pelos usuários de certificados

O usuário é responsável pelos danos que der causa à AC Raiz.

2.3.2. Relações Fiduciárias

A AC Raiz responde pelos danos que der causa.

2.3.3. Processos Administrativos

Não se aplica.

2.4. Interpretação e Execução

2.4.1. Legislação

Esta DPC é regida pela Medida Provisória Nº 2.200-2, bem como pelas demais leis em vigor no Brasil.

2.4.2. Forma de interpretação e notificação (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

Na hipótese de uma ou mais das disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável por lei, tal inaplicabilidade não afetará as demais disposições, sendo esta DPC interpretada então como se não contivesse tal disposição, e na medida do possível, interpretada para manter a intenção original da DPC.

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis.

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, 5 preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

2.4.3. Procedimentos de solução de disputa

No caso de um conflito entre esta DPC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e renovação de certificados

As tarifas de emissão e de renovação de certificado pela AC Raiz serão definidas de acordo com as regras estipuladas pelo CG da ICP-Brasil.

A única forma de renovação de certificado realizada pela AC Raiz é aquela descrita no item 3.2.

2.5.2. Tarifas de acesso ao certificado

Não se aplica.

2.5.3. Tarifas de revogação ou de acesso à informação de status

A tarifa de revogação de certificado pela AC Raiz, por solicitação da AC titular do certificado, será definida de acordo com as regras estipuladas pelo CG da ICP-Brasil.

Não há tarifa de acesso a informação de status de certificado gerenciada pela AC Raiz.

2.5.4. Tarifas para outros serviços, tais como informação de política

Tarifas para outros serviços da AC Raiz serão definidas de acordo com as regras estipuladas pelo CG da ICP-Brasil.

2.5.5. Política de reembolso

Não se aplica.

2.6 Publicação e Repositório

2.6.1. Publicação de informação da AC Raiz (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

O certificado da AC Raiz, sua LCR e os certificados das AC de nível imediatamente subsequente ao seu são publicados em serviço de diretório 6 e/ou em página *Web* da AC Raiz, obedecendo as regras e os critérios estabelecidos nesta DPC.

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

A disponibilidade das informações publicadas pela AC Raiz em serviço de diretório e/ou 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.

A AC Raiz inclui nos certificados emitidos a identificação da sua página *Web*.

2.6.2. Frequência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação de LCR se dá conforme o item 4.4.9.

2.6.3. Controles de acesso

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

São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação dessas informações a pessoal autorizado.

2.6.4. Repositórios

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

dias por semana.

2.7. Auditoria de Conformidade

A auditoria realizada pela AC Raiz importa em verificar se todos os processos, procedimentos e atividades das AC integrantes da ICP-Brasil e suas AR estão em conformidade com as suas respectivas DPC, suas Políticas de Certificado, a Política de Segurança e as demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.1. Frequência de auditoria de conformidade de AC (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

As AC integrantes da ICP-Brasil sofrem auditoria:

- previamente ao seu credenciamento na ICP-Brasil; e
- a qualquer tempo, sem aviso prévio.

Adicionalmente, as AC de nível imediatamente subsequente ao da AC Raiz sofrem auditoria anualmente, para fins de continuidade do credenciamento.

2.7.2. Identidade e qualificação do auditor (REDAÇÃO DADA PELA RESOLUÇÃO 13, DE 26 DE ABRIL DE 2002)

A auditoria será realizada por corpo próprio devidamente qualificado e vinculado à AC Raiz.

2.7.3. Relação entre auditor e parte auditada

O auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta DPC, aplicam-se, no que couber, as regras de suspeição e impedimento estabelecidas nos arts. 134º e 135º do Código de Processo Civil

O auditor será declarado impedido de realizar auditoria, quando:

- houver motivo íntimo declarado;
- for amigo íntimo ou inimigo capital de membros da AC auditada;
- for credor ou devedor da AC auditada ou de um de seus membros;
- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços;
- tiver interesse no resultado da auditoria da AC auditada; e
-
- houver relacionamento, de fato ou de direito, como cônjuge, parente, consanguíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.
-

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer das causas de impedimento.

2.7.4. Tópicos cobertos pela auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Todos os eventos significativos ocorridos em um sistema de AC ou de AR devem ser armazenados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.

Os tópicos cobertos por uma auditoria de conformidade incluem, dentre outros:

- Política de Segurança;
- Segurança física;

- Avaliação de tecnologia;
- Administração dos serviços;
- Investigação de pessoal;
- PC e DPC utilizadas;
- Contratos;
- Considerações de sigilo.

2.7.5. Medidas a serem adotadas em caso de não conformidade (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

Cabe à entidade auditada cumprir, no prazo estipulado pela AC Raiz da ICP-Brasil, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará o cancelamento do credenciamento da entidade auditada, salvo determinação contrária da AC Raiz da ICP-Brasil.

Cabe à AC Raiz tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-Brasil, podendo cancelar imediatamente o credenciamento da AC e da AR auditada, mediante decisão motivada.

A AC Raiz, em casos de iminente dano irreparável ou de difícil reparação a terceiros, suspenderá cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subsequente ao seu.

2.7.6. Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada e à AC Raiz.

2.8. Sigilo

A chave privada de assinatura digital de cada AC credenciada é gerada e mantida pela própria AC, que deve assegurar seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC é de sua inteira responsabilidade.

2.8.1. Tipos de informações sigilosas (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

Como princípio geral, todo documento, informação ou registro fornecido à AC Raiz será sigiloso.

2.8.2. Tipos de informações não sigilosas (RESOLUÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

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

Os seguintes documentos da AC Raiz e das AC de nível imediatamente subsequente ao seu também são considerados documentos não sigilosos:

- qualquer PC aplicável;
- qualquer DPC;
- versões públicas de Políticas de Segurança;
- a conclusão dos relatórios da auditoria.

2.8.3. Divulgação de informação de revogação/suspensão de certificado

Informações sobre revogação de certificados de AC de nível imediatamente subsequente ao da AC Raiz são fornecidas na LCR da AC Raiz. As razões para a revogação de certificado serão tornadas públicas.

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.4. Quebra de sigilo por motivos legais

Mediante ordem judicial, serão fornecidos quaisquer documentos, informações ou registros sob a guarda da AC Raiz.

2.8.5. Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC Raiz será fornecido a qualquer pessoa, exceto quando a pessoa que requerer, através de instrumento devidamente constituído, seja autorizada para fazê-lo e esteja corretamente identificada.

2.8.6. Divulgação por solicitação do titular

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

Autorizações formais podem ser apresentadas de duas formas:

- por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
- por meio de pedido escrito com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal.

2.8.7. Outras circunstâncias de divulgação de informação

Não se aplica.

2.9. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. Registro Inicial

3.1.1. Tipos de nomes

As AC de nível imediatamente subsequente ao da AC Raiz, titulares de certificados, terão um nome que as identifiquem univocamente no âmbito da ICP-Brasil.

3.1.2. Necessidade de nomes significativos

Todos os certificados emitidos pela AC Raiz da ICP-Brasil devem incluir um identificador único que represente a AC de nível imediatamente subsequente para a qual o certificado foi emitido, conforme item 7.2.4.

3.1.3. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.4. 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 X.509. A extensão “*Unique Identifiers*” não será admitida para diferenciar as AC com nomes idênticos.

3.1.5. Procedimento para resolver disputa de nomes

A AC Raiz reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das AC 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.

3.1.6. Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7. Método para comprovar a posse de chave privada (REDAÇÃO DADA PELA RESOLUÇÃO Nº 04, DE 22 DE NOVEMBRO DE 2001)

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 2510 é utilizada para essa finalidade.

3.1.8. Identificação de uma organização

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.

3.1.9. Autenticação da identidade de um indivíduo

Não se aplica.

3.2. Criação de novo par de chaves antes da expiração do atual (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

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 do certificado vigente da AC. Para isto, um representante legal da AC deve preencher e assinar digitalmente o formulário eletrônico Revalidação dos Dados Cadastrais e Solicitação de Novo Certificado. 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. Criação de novo par de chaves após revogação (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

A solicitação de novo certificado de AC após a revogação do certificado anterior deverá ser efetivada pelo preenchimento do formulário Revalidação dos Dados Cadastrais e Solicitação de Novo Certificado. Este 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. Solicitação de Revogação

O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.4.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subsequente ao da AC Raiz. O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.4.3. Solicitações de revogação de certificados devem ser documentadas.

4. REQUISITOS OPERACIONAIS

4.1. Solicitação de Certificado (REDAÇÃO DADA PELA RESOLUÇÃO 13, DE 26 DE ABRIL DE 2002)

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 (Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil).

A AC deve encaminhar a solicitação de seu certificado à AC Raiz por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10².

² PKCS (*Public Key Cryptographic Standards*), RSA Data Security.

4.2. Emissão de Certificado (REDAÇÃO DADA PELA RESOLUÇÃO 37, DE 21 DE OUTUBRO DE 2004)

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

A AC Raiz garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 20 (vinte) dias úteis após a autorização de funcionamento da AC em questão.

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

A AC Raiz entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC credenciada.

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

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

- 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;
- à formalização do contrato administrativo e ao pagamento da tarifa a que se referem os artigos 1º e 2º da Resolução Nº 10, de 14 de fevereiro de 2002.

Os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, que respondem na forma do art. 37, §6º, da Constituição Federal, ficam dispensados da apresentação da apólice prevista neste item.”

4.3. Aceitação de Certificado

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.

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 Acordo por seu representante legal. 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. 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.

Ao aceitar o certificado, a AC titular:

- concorda com as responsabilidades, obrigações e deveres a ela impostas pelo Termo de Acordo e esta DPC;
- garante que com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada com o certificado;
- 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.

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. Suspensão e Revogação de Certificado

4.4.1. Circunstâncias para revogação (REDAÇÃO DADA PELA RESOLUÇÃO 21, DE 29 DE AGOSTO DE 2003)

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.

Um certificado deve obrigatoriamente ser revogado:

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

A AC Raiz da ICP-Brasil 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.

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

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

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

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

4.4.2. Quem pode solicitar revogação

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

- por determinação da AC Raiz ou do CG da ICP-Brasil; ou
- por solicitação da AC titular do certificado.

4.4.3. Procedimento para solicitação de revogação (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

A solicitação de revogação do certificado à AC Raiz deve ser efetivada pelo preenchimento do formulário Solicitação de Revogação de Certificado de AC. 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.

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 ao CG da ICP-Brasil e à AC afetada a revogação do certificado.

O prazo para a revogação de certificado de AC de nível imediatamente subsequente ao da AC Raiz conta-se, inclusive nos casos de solicitação da AC titular do certificado, da determinação da AC Raiz ou do CG da ICP-Brasil e deve ser realizada em até 2 (duas) horas.

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.

4.4.4. Prazo para solicitação de revogação

A solicitação de revogação deve ser imediata quando configuradas circunstâncias definidas no item 4.4.1 desta DPC.

Quando a solicitação de revogação é feita pela AC titular do certificado dentro do prazo de aceitação definido no item 4.3, nenhuma tarifa é cobrada da AC solicitante.

4.4.5. Circunstâncias para suspensão

Não é permitida, no âmbito da ICP-Brasil, a suspensão de certificados de AC de nível imediatamente

subseqüente ao da AC Raiz.

4.4.6. Quem pode solicitar suspensão

Não se aplica.

4.4.7. Procedimento para solicitação de suspensão

Não se aplica.

4.4.8. Limites no período de suspensão

Não se aplica.

4.4.9. Frequência de emissão de LCR (REDAÇÃO DADA PELA RESOLUÇÃO 13, DE 26 DE ABRIL DE 2002)

A LCR da AC Raiz é atualizada a cada 28 (vinte e oito) dias. Em caso de revogação de certificado de AC de nível imediatamente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.4.3 e notifica todas as AC de nível imediatamente subseqüente ao seu.

4.4.10. Requisitos para verificação de LCR

Todos os certificados das AC de nível imediatamente subseqüente 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.

4.4.11. 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.

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

Não aplicável.

4.4.13. Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC Raiz também podem ser divulgadas por meio de sua publicação no Diário Oficial da União ou na página *Web* da AC Raiz.

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

As formas de verificação de revogação descritas no item anterior são meramente informativas.

4.4.15. Requisitos especiais para o caso de comprometimento de chave

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

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.

4.5. Procedimentos de Auditoria de Segurança

4.5.1. Tipos de eventos registrados

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.

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 no arquivo de auditoria:

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

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

- registros de acessos físicos;
- manutenção e mudanças na configuração dos seus sistemas;
- mudanças de pessoal;
- relatórios de discrepância e comprometimento; e
- registros de destruição de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuário.

Para facilitar o processo de auditoria, toda a documentação relacionada aos serviços da AC Raiz é coletada e consolidada, eletrônica ou manualmente, num local único, conforme a Política de Segurança da ICP-Brasil.

4.5.2. Frequência de auditoria de registros

AC Raiz garante que seus registros de auditoria são analisados mensalmente, sempre que houver utilização de seu sistema de certificação (equipamento *off-line*, que permanece desligado grande parte do tempo) ou em caso de suspeita de comprometimento da segurança. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nos mesmos.

Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3. Período de retenção para registros de auditoria

A AC Raiz mantém em suas próprias instalações os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, os armazena da maneira descrita no item 4.6.

4.5.4. Proteção de registros de auditoria

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.

4.5.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

Os registros de eventos e sumários de auditoria do equipamento *off-line* utilizado pela AC Raiz têm cópias de segurança mensais ou sempre que houver alguma utilização desse equipamento.

4.5.6. Sistema de coleta de dados de auditoria

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.

4.5.7. 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 causou o evento.

4.5.8. Avaliações de vulnerabilidade

Os eventos que representem possível vulnerabilidade, detectados na análise mensal 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.

4.6. Arquivamento de Registros

4.6.1. Tipos de registros arquivados (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

Informações de auditoria detalhadas no item 4.5.1 e os processos de credenciamento de AC de nível imediatamente subsequente ao da AC Raiz.

4.6.2. Período de retenção para arquivo

Eventos relacionados no item anterior são retidos por, no mínimo, 06 (seis) anos.

4.6.3. Proteção de arquivo

Todos os arquivos são protegidos e armazenados fisicamente com os mesmos requisitos de segurança que os de sua instalação.

4.6.4. Procedimentos de registros de arquivo

Uma segunda cópia de todo o material descrito no item 4.6.1 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 verifica a integridade das cópias de segurança a cada 6 (seis) meses.

4.6.5. Requisitos para datação (*time-stamping*) de registros (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time* (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos é zero.

4.6.6. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Raiz em seus procedimentos operacionais são internos.

4.6.7. Procedimentos para obter e verificar informação de arquivo

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.

4.7. Troca de chave

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.

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 por, no mínimo, 30 (trinta) anos para efeito de consulta histórica.

4.8. Comprometimento e Recuperação de Desastre

A AC Raiz possui um plano de continuidade do negócio, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

4.8.1. Recursos computacionais, *software*, e/ou dados corrompidos

Procedimentos descritos no Plano de Continuidade do Negócio da AC Raiz.

4.8.2. Revogação de certificado da entidade (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

Procedimentos descritos no Plano de Continuidade do Negócio da AC Raiz.

4.8.3. Comprometimento de chave de entidade

Procedimentos descritos no Plano de Continuidade do Negócio da AC Raiz.

4.8.4. Segurança dos recursos após desastre de qualquer espécie

Procedimentos descritos no Plano de Continuidade do Negócio da AC Raiz.

4.9. Extinção da AC Raiz

No caso de extinção da AC Raiz, devem ser tomadas, no mínimo, as seguintes providências:

- notificação de todas as entidades integrantes da ICP-Brasil;
- manutenção da operação da AC Raiz pelo período mínimo de 1 (um) ano após a notificação de sua extinção, salvo em casos de sucessão;
- armazenamento dos dados da AC Raiz pelo período previsto na legislação.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

5.1. Controles Físicos

5.1.1. Construção e localização das instalações

Os serviços da AC Raiz são realizados pelo Instituto Nacional de Tecnologia da Informação ITI, em instalações homologadas pelo Comitê Gestor (CG) da ICP-Brasil.

5.1.2. Acesso físico

O acesso físico às dependências da AC Raiz é gerenciado e controlado internamente conforme o previsto na Política de Segurança da ICP-Brasil. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso. O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes.

O sistema de certificação da AC Raiz está situado em uma sala-cofre, localizada nas suas instalações. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.3. Energia e ar condicionado

A sala-cofre da AC Raiz, além de conectada à rede elétrica, dispõe dos seguintes recursos, que permitem sua operação ininterrupta, mesmo em caso de interrupção no fornecimento de energia:

- gerador de porte compatível;
-
- gerador de reserva;
- sistema de *no-breaks*;
-
- sistema de aterramento e proteção a descargas atmosféricas;
-
- iluminação de emergência.
-

A área tem um sistema de ar condicionado tolerante a falhas que controla calor e umidade, independente do sistema de ar condicionado do edifício onde está localizado.

5.1.4. Exposição à água

A sala-cofre é construída na forma de uma célula estanque, inteiriça, imune a infiltrações e inundações.

5.1.5. Prevenção e proteção contra incêndio

A sala-cofre possui sistema para detecção antecipada de fumaça através de partículas iônicas e sistema de extinção de incêndio por gás.

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

5.1.6. Armazenamento de mídia

Para garantir a segurança de mídia armazenada, a AC Raiz dispõe de ambientes específicos que garantem que as mídias neles armazenadas não sofram nenhum tipo de dano gerado por fatores externos.

5.1.7. Destruição de lixo

Todos os documentos em papel com informações sensíveis são destruídos antes de ir para o lixo.

Todos os dispositivos eletrônicos não mais utilizáveis, que tenham sido anteriormente utilizados no armazenamento de informações sensíveis, são fisicamente destruídos.

5.1.8. Sala externa de arquivos (*off-site*)

Uma sala de armazenamento externa à AC Raiz é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala está disponível a pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e tem níveis apropriados de segurança física implementados.

5.2. Controles Procedimentais

5.2.1. Perfis qualificados (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

A AC Raiz garante a separação das tarefas para funções críticas, com o intuito de evitar que um empregado de má fé utilize o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

A AC Raiz estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. A divisão de responsabilidades entre os três perfis é a seguinte:

Gerente de Configurações:

- configuração e manutenção do *hardware* e do *software* da AC Raiz;
- início e término dos serviços da AC Raiz;

–
Gerente de Segurança:

- gerenciamento dos operadores da AC Raiz;
- implementação das políticas de segurança da AC Raiz;
- verificação dos registros de auditoria;
- verificação do cumprimento desta DPC;

Administrador do Sistema:

- gerenciamento dos processos de iniciação dos usuários internos à AC Raiz;
-
- emissão, expedição, distribuição, revogação e gerenciamento de certificados;
- distribuição de cartões (*tokens*), quando for o caso.

Somente os empregados responsáveis por tarefas descritas para o Gerente de Configurações e o Administrador do Sistema têm acesso ao *software* e ao *hardware* do sistema de certificação da AC Raiz.

5.2.2. Número de pessoas necessário por tarefa

Controle multiusuário é requerido para a geração e a utilização da chave privada da AC Raiz, conforme o descrito em 6.2.2.

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Raiz necessitam da presença de no mínimo 2 (dois) empregados da AC Raiz. As demais tarefas da AC Raiz podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

Todo empregado da AC Raiz tem sua identidade e perfil verificados antes de:

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

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

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

5.3. Controles de Pessoal

Todos os empregados da AC Raiz que executam tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- os termos e as condições do perfil que ocupam;
-
- o compromisso de não divulgar informações sigilosas a que têm acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão,

expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da ICP-Brasil.

5.3.2. Procedimentos de verificação de antecedentes

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

- verificação de antecedentes criminais;
- verificação de situação de crédito;
- verificação de histórico de empregos anteriores;
- comprovação de escolaridade e de residência;
-
- assinatura de termos de sigilo e de responsabilidade específicos.
-

5.3.3. Requisitos de treinamento

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:

- princípios e mecanismos de segurança da AC Raiz;
- *software* de certificação em uso na AC Raiz;
- atividades sob sua responsabilidade; e
- procedimentos de recuperação de desastres e de continuidade do negócio.

5.3.4. Frequência e requisitos para reciclagem técnica

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. Treinamentos de reciclagem são realizados pela AC Raiz sempre que há a necessidade.

5.3.5. Frequência e seqüência de rodízio de cargos

Não estipuladas.

5.3.6. Sanções para ações não autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC Raiz suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC Raiz no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na Política de Segurança da ICP-Brasil.

5.3.8. Documentação fornecida ao pessoal

A AC Raiz disponibiliza para todo o seu pessoal:

- sua DPC;
- a Política de Segurança da ICP-Brasil;
- documentação operacional relativa a suas atividades;

-
- contratos, normas e políticas relevantes para suas atividades.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

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

O par de chaves criptográficas da AC Raiz é gerado pela própria AC Raiz, em *hardware* específico, conforme o detalhado em 6.1.8.

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 conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

A AC de nível imediatamente subsequente ao da AC Raiz entrega à AC Raiz cópia de sua chave pública, em formato PKCS#10. 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. Disponibilização de chave pública da AC Raiz para usuário (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

A entrega do certificado da AC Raiz para as AC de nível imediatamente subsequente ao seu é feita no momento da disponibilização do certificado da AC, utilizando-se para isto o formato padrão PKCS#7, que inclui toda a cadeia de certificação.

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

- formato PKCS#7, na disponibilização do certificado para seu titular;
-
- diretório;
-
- página *Web* da AC Raiz ou das AC integrantes da ICP-Brasil;
-
- 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 AC de nível imediatamente subsequente ao seu é de, no mínimo 2048 (dois mil e quarenta e oito) bits, devendo este valor ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC Raiz adotam o padrão FIPS 140-1³, *level 3*, conforme estabelecido pelo CG da ICP-Brasil.

6.1.7. Verificação da qualidade dos parâmetros

Parâmetros verificados de acordo com as normas estabelecidas pelo CMVP⁴.

³ FIPS 140-1 - Federal Information Processing Standards 140-1. Este padrão será substituído pelo pelo FIPS 140-2, hoje em fase de implantação por parte do National Institute of Standards and Technology.

⁴ CMVP (Cryptographic Module Validation Program)

6.1.8. Geração de chave por *hardware/software*

A AC Raiz utiliza um componente seguro de *hardware* para a geração de seu par de chaves, de seu certificado, dos certificados das AC de nível imediatamente subsequente ao seu e para a geração e assinatura de sua LCR. O componente seguro de *hardware* utiliza um mecanismo de detecção de violação.

6.1.9. 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 AC de nível imediatamente subsequente ao seu e de sua LCR.

6.2. Proteção da Chave Privada

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 para módulo criptográfico

O módulo criptográfico da AC Raiz adota o padrão FIPS 140-1, *level 3*, conforme estabelecido pelo CG 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. Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) das chaves privadas da AC Raiz ou das AC de nível imediatamente subsequente.

6.2.4. Cópia de segurança de chave privada

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.

A AC Raiz não mantém cópia de segurança das chaves privadas das AC 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 (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

A chave privada da AC Raiz é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7. 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*).

6.2.8. 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.

6.2.9. Método de destruição de chave privada

Além do estabelecido no item 6.2.8, todas as cópias de segurança da chave privada da AC Raiz devem ser destruídas.

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 AC de nível imediatamente subsequente ao seu permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2. 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

A geração do par de chaves da AC Raiz e dos certificados das AC 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.

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

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

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

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. O *software* de certificação da AC Raiz é instalado pelo próprio fabricante. Novas versões desse *software* somente serão instaladas após comunicação do fabricante e testes em ambiente de homologação da AC Raiz.

6.6.3. Classificações 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. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado para armazenamento da chave privada da AC Raiz está em conformidade com o padrão FIPS 140-1, *level 3*, conforme estabelecido pelo CG da ICP-Brasil.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil de Certificado da AC Raiz (REDAÇÃO DADA PELA RESOLUÇÃO Nº 34 DE 21 DE OUTUBRO DE 2004)

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

O certificado da AC Raiz é o único certificado auto-assinado da ICP-Brasil, e possui validade de 13 (treze) anos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

7.1.1. Número de versão

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

7.1.2. Extensões de certificado (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

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

- **basicConstraints**: contém o campo *cA=True*. O campo *pathLenConstraint* não é utilizado.
- **keyUsage**: contém apenas os bits *keyCertSign(5)* e *cRLSign(6)* ligados. Os demais bits estão desligados.
- **cRLDistributionPoints**: contém o endereço na *Web* onde se obtém a LCR emitida pela AC Raiz (<http://acraiz.icpbrasil.gov.br/LCRacraiz.crl>).

- **Certificate Policies:** especifica o *Object Identifier* (OID) da DPC da AC Raiz e o atributo *id-qt-cps* com o endereço na *Web* dessa DPC (<http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf>).
- **SubjectKeyIdentifier:** contém o *hash* SHA-1 da chave pública da AC Raiz.

7.1.3. Identificadores de algoritmo

O certificado da AC Raiz é assinado com o uso do algoritmo RSA com SHA-1 como função *Hash*, conforme o padrão PKCS#1.

7.1.4. Formatos de nome

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 X.500/ISO 9594, como abaixo descrito:

C = BR
 O = ICP-Brasil
 OU = Instituto Nacional de Tecnologia da Informação - ITI
 CN = Autoridade Certificadora Raiz Brasileira

7.1.5. Restrições de nome

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

7.1.6. OID (*Object Identifier*) da DPC

A ser definido pela AC Raiz.

7.1.7. Uso da extensão “*Policy Constraints*”

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.1.9. Semântica de processamento para as extensões críticas de Política de Certificado

Não se aplica.

7.2. Perfil de Certificado da AC de nível subsequente ao da AC Raiz (REDAÇÃO DADA PELA RESOLUÇÃO Nº 34 DE 21 DE OUTUBRO DE 2004)

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

O certificado da AC de nível subsequente ao da AC Raiz é assinado pela AC Raiz, e possui validade de no máximo 8 (oito) anos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

7.2.1. Número(s) de versão

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

7.2.2. Extensões de certificado

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

7.2.3. Identificadores de algoritmo

O certificado de AC de nível subsequente ao da AC Raiz é assinado com o uso do algoritmo RSA com o SHA-1 como função *Hash*, conforme o padrão PKCS#1.

7.2.4. Formatos de nome

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 X.500/ISO 9594, da seguinte forma:

DN do titular:

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

DN do emissor:

C = BR
O = ICP-Brasil
OU = Instituto Nacional de Tecnologia da Informacao - ITI
CN = Autoridade Certificadora Raiz Brasileira

7.2.5. Restrições de nome (REDAÇÃO DADA PELA RESOLUÇÃO 13, DE 26 DE ABRIL DE 2002)

O nome da AC titular do certificado deve ser submetido à aprovação no processo de credenciamento. Não são admitidos caracteres especiais ou de acentuação nos campos do DN.

7.2.6. OID (*Object Identifier*) da DPC (REDAÇÃO DADA PELA RESOLUÇÃO 04, DE 22 DE NOVEMBRO DE 2001)

A AC de nível imediatamente subsequente ao da AC Raiz deve informar neste item o OID fornecido para sua DPC pela AC Raiz.

7.2.7. Uso da extensão “*Policy Constraints*”

Não se aplica.

7.2.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.2.9. Semântica de processamento para as extensões críticas de Política de Certificado

Não se aplica.

7.3. Perfil de LCR

7.3.1. Número(s) de versão

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

7.3.2. Extensões de LCR e de suas entradas (REDAÇÃO DADA PELA RESOLUÇÃO Nº 04, DE 22 DE NOVEMBRO DE 2001)

A LCR emitida pela AC Raiz implementa as seguintes extensões previstas na RFC 2459:

- **AuthorityKeyIdentifier**: contém o mesmo valor do campo “*Subject Key Identifier*” do certificado da AC Raiz.
- **cRLNumber**: contém um número seqüencial para cada LCR emitida.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC deverá ser submetida pela AC Raiz à aprovação do CG da ICP-Brasil.

8.2. Políticas de publicação e notificação

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

8.3. Procedimentos de aprovação da DPC

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

ALTERADA EM 22.11.2001 PELA RESOLUÇÃO 04.
ALTERADA EM 14.02.2002 PELA RESOLUÇÃO 11.
ALTERADA EM 26.04.2002 PELA RESOLUÇÃO 13.
ALTERADA EM 29.08.2003 PELA RESOLUÇÃO 21.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 34.
ALTERADA EM 21.12.2004 PELA RESOLUÇÃO 37.
REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 38