RESOLUÇÃO Nº 151, DE 30 DE MAIO DE 2019

Regulamenta requisitos para conformidade ao Programa WebTrust de Princípios e Critérios para as entidades da ICP-Brasil e simplifica processos da ICP-Brasil.

O COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no uso das atribuições que lhe confere o art. 6º, §1º, inc. IV, do Regimento Interno, torna público que o COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício das competências previstas no art. 4º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, em reunião ordinária realizada em 30 de maio de 2019,

CONSIDERANDO a previsão expressa no art. 653 do Código Civil de que a procuração é instrumento de mandato por meio do qual alguém recebe de outrem poderes para, em seu nome, praticar atos ou administrar interesses,

CONSIDERANDO a necessidade de manter a conformidade com o Programa WebTrust de Princípios e Critérios para Autoridades de Certificação,

CONSIDERANDO a oportunidade para a simplificação dos processos e redução de custos na infraestrutura da ICP-Brasil, e

CONSIDERANDO a necessidade de prever que os serviços de gestão do ciclo de vida de certificados de atributo possam ser providos no âmbito de Prestadores de Serviço de Confiança na modalidade de portal de assinaturas,

RESOLVEU:

Art. 1º O § 5º do art. 24 da Resolução nº 137, de 8 de março de 2018, passa a vigorar com a seguinte redação:

"……...

§5º Caso não seja possível a participação do titular e de seu suplente, o membro titular poderá indicar representante, desde que outorgada procuração, assinada digitalmente, que contenha o assunto referente da pauta e o teor do voto, que constará na ata da reunião.

……" (NR)

Art. 2º O DOC-ICP-02, versão 3.0, passa a vigorar com as seguintes alterações:

"…….

6.2. Gerenciamento de Riscos

O processo de gerenciamento de riscos deve ser revisto anualmente pela própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.

……...

6.4.2 Todas as ACs deverão apresentar, ainda, Plano de Recuperação de Desastres e Plano de Resposta a Incidentes a serem aprovados pela AC Raiz ou AC de nível imediatamente superior.

……...

7.3.1 O Processo de Admissão

7.3.1.1 Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.

7.3.1.2 Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

7.3.1.3 O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICP-Brasil.

……...

7.3.3 O Levantamento de Dados Pessoais

Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil, verificação de antecedentes e verificação de grau de instrução.

……...

7.4.4……..……..

i) manter registros de atividades de usuários de TI (*logs*) por um período de no mínimo 7 (sete) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.);

……...

9.3.2.5.Proteção lógica adicional (criptografia) deve ser adotada, quando necessária, para evitar o acesso não-autorizado às informações.

……...

9.3.3.28. As chaves privadas das ACs deverão estar protegidas de acesso desautorizado, para garantir seu sigilo e integridade.

……...

12.2 ……..……...

g) reavaliação periódica dos riscos em intervalos de tempo não superiores a um ano.

…….

13.2.2. Todas as ACs e ACTs integrantes da ICP-Brasil deverão apresentar um PCN e, ainda, um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres, que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

1. As condições para ativar o plano;
2. Procedimentos de emergência;
3. Procedimentos de fallback;
4. Procedimentos de restauração;
5. Cronograma para manutenção do plano;
6. Requisitos de conscientização e educação;
7. Responsabilidades individuais;

8. Objetivo de Tempo de Recuperação (RTO);

9. Testes regulares dos planos de contingência;

10. O plano para manter ou restaurar as operações de negócios da AC de forma oportuna, após a interrupção ou falha de processos críticos de negócios;

11. Definição de requisitos para armazenar materiais criptográficos críticos em um local alternativo;

12. Definição de interrupções aceitáveis do sistema e um tempo de recuperação;

13. Frequência para realização de cópias de backup;

14. Distância entre as instalações de recuperação e o site principal da AC; e

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

No tratamento constante nos Planos acima, deve ser considerado:

a) comprometimento da chave privada das entidades;

b) invasão do sistema e da rede interna da entidade;

c) incidentes de segurança física e lógica;

d) indisponibilidade da Infraestrutura;

e) fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados;

f) comprometimento de controle de segurança em qualquer evento referenciado no PCN;

g) notificação à comunidade de usuários, se for o caso;

h) revogação dos certificados afetados, se for o caso;

i) procedimentos para interrupção ou suspensão de serviços e investigação;

j) análise e monitoramento de trilhas de auditoria; e

k) com o público e com meios de comunicação, se for o caso.

……..” (NR)

Art. 3º O item 4 do DOC-ICP-06, versão 3.1, passa a vigorar com a seguinte redação:

“4 **-** Os órgãos e entidades da Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios, bem como suas autarquias e fundações públicas, estão dispensados do pagamento das tarifas a que se referem os itens 1 a 3 deste documento.” (NR)

Art. 4º O DOC-ICP-08, versão 4.5, passa a vigorar com as seguintes alterações:

“……

1.4 Toda correspondência tratada neste documento deve ser formalizada, preferencialmente, por meio de correio eletrônico, em formato PDF, com assinatura digital ICP-Brasil da autoridade competente. Os arquivos devem ter calculados os respectivos hashes, com algoritmo SHA-1, cujos valores serão relacionados em arquivo no formato texto puro (extensão TXT), contendo o nome do arquivo e o respectivo hash, separados por ponto e vírgula (;).

……..

2.1 As auditorias são classificadas em **PRÉ-OPERACIONAIS** e **OPERACIONAIS**, a saber:

a) **Pré-operacionais**: são as auditorias realizadas antes do início das atividades do candidato a Prestador de Serviço de Certificação (PSCert), quer seja Autoridade Certificadora (AC), Autoridade de Carimbo do Tempo (ACT), Autoridade de Registro (AR), Prestador de Serviço de Suporte (PSS), Prestador de Serviço Biométrico (PSBio) ou PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas; e

b) **Operacionais**: são as auditorias realizadas anualmente, considerado o ano civil, em todos os PSCert para manutenção do credenciamento junto à ICP-Brasil. Tais auditorias ocorrerão a partir do primeiro ano civil seguinte à data da publicação no DOU do credenciamento do PSCert.

…….

3.1…….

ENTIDADE	**EXECUTOR DA AUDITORIA**	
	Pré-operacional	**Operacional**
AC Raiz	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados	Comitê Gestor da ICP-Brasil ou seus prepostos, formalmente designados
AC de 1º Nível[1], e seus PSS	ITI/DAFN/CGAFI	ITI/DAFN/CGAFI
AC subsequente[2] e seus PSS	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
ACT	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
AR	AC ou PSS credenciados junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI	Auditoria Interna da respectiva AR credenciada junto ao ITI AC ou PSS credenciados junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
AR no Exterior	ITI/DAFN/CGAFI ou, a seu critério, AC ou PSS credenciados junto ao ITI	AC ou PSS credenciados junto ao ITI Auditoria Interna da respectiva AR credenciada junto ao ITI Empresa de Auditoria Independente credenciada junto ao ITI
PSBio	ITI/DAFN/CGAFI	Empresa de Auditoria Independente credenciada junto ao ITI
PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas	ITI/DAFN/CGAFI	Empresa de Auditoria Independente, credenciada junto ao ITI

……..

4.7 O pedido de credenciamento deve ser encaminhado ao Protocolo Geral da AC Raiz, assinado pela entidade candidata, anexando os arquivos eletrônicos, conforme item 1.4.

4.8 O ITI poderá solicitar a complementação da documentação, só voltando a ser contado o prazo a partir do recebimento do que for solicitado.

4.9 Se a solicitação não for atendida em até 15 dias, o processo será arquivado, mediante despacho fundamentado da DAFN.

4.10 A documentação apresentada pela candidata para credenciamento constituirá processo específico, por prazo não inferior a 5 (cinco) anos, exceto quanto à eventual documentação de auditorias realizadas, que será considerada confidencial, ficando à disposição apenas dos próprios solicitantes do credenciamento.

4.11 Sobre o pedido de credenciamento ou de renovação, o Diretor da DAFN, por meio de despacho fundamentado, poderá:

a) deferir o pedido;

b) notificar a candidata para, no prazo máximo de 15 (quinze) dias corridos, complementar a documentação apresentada;

c) indeferir o pedido se, vencido o prazo da alínea "b", não forem cumpridas as exigências constantes da notificação retromencionada; e

d) indeferir o pedido que não atenda aos requisitos técnicos estabelecidos.

……

4.15 Qualquer alteração ocorrida, quer seja em atos constitutivos, estatuto, contrato social, organograma ou vinculação da entidade, quer seja dos dirigentes ou da equipe técnica de auditores, será submetida imediatamente ao conhecimento da DAFN, mediante formalização protocolada no Protocolo Geral da AC Raiz e que fará parte do processo de credenciamento da respectiva entidade de auditoria. Nestes casos será reavaliada a manutenção das condições exigidas para o credenciamento, observadas as regras para as renovações, podendo ser dispensada a apresentação de certidões ainda não exigíveis.

…….

5 PLANO ANUAL DE AUDITORIA OPERACIONAL (PLAAO)

5.1 Cada AC e ACT protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, contemplando todos os PSCert diretamente subordinados (AC subsequente e AR), por meio do formulário ADE-ICP-08-C[4].

5.2 As auditorias operacionais serão realizadas anualmente nos seguintes PSCert:

a) AC credenciada e respectivos PSS;

b) ACT credenciada e respectivos PSS;

c) AR credenciada.

5.3 Cada PSBio protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, contemplando os PSS subordinados, por meio do formulário ADE-ICP-08-C[4].

5.4 Cada PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas protocolará no Protocolo Geral da AC Raiz, até o dia 15 (quinze) de dezembro de cada ano, para conhecimento da DAFN, seu PLAAO para o ano civil seguinte, por meio do formulário ADE-ICP-08.C [4].

…….

6.1.1 As auditorias têm por objetivo avaliar se os processos, procedimentos, atividades e controles estão em conformidade com as respectivas Políticas, Declaração de Práticas, Política de Segurança e demais normas e procedimentos estabelecidos pelo Comitê Gestor da ICP-Brasil. O documento ADE-ICP-08-E[5] detalha os processos que compõem a cadeia de certificação e deverá nortear as auditorias realizadas na cadeia da ICP-Brasil. Adicionalmente, as auditorias do tipo 1 também devem avaliar os princípios e critérios definidos pelo WebTrust.

……..

6.1.12 No caso de uma AC optar por auditar com seus profissionais suas AR, deverá observar o disposto nos itens acima, excetuados os itens 6.1.5 e 6.1.6.

…….

7.1 Aplica-se ao auditor independente, no que couber, as regras de suspeição e impedimento estabelecidas nos artigos 134 e 135 do Código de Processo Civil; além das demais normas para o exercício da profissão de auditor independente ou interno.

……..

7.7 Ocorrendo o impedimento da entidade de auditoria, esta deverá concluir os trabalhos cujas atividades de campo já tenham iniciado, estando impedida de iniciar novos trabalhos de campo.

a) Eventuais relatórios de auditoria recebidos em desacordo com o caput serão sumariamente arquivados e não terão nenhuma validade perante o ITI, no que se refere ao cumprimento da obrigatoriedade de realização de auditorias.

……

8.2 A documentação de auditoria será avaliada em comparação com a metodologia de auditoria aprovada no credenciamento da entidade de auditoria, exceto quando realizado por AC ou PSS diretamente em suas AR.

……

9.6 No ITI, os casos de não-conformidade que ensejaram recomendações à entidade auditada serão acompanhados pela área de auditoria e incluídos nos planos de trabalho de auditorias posteriores na mesma entidade.

…….

9.10 A entidade cujo conceito atribuído seja cinco (5) – INACEITÁVEL – em duas auditorias operacionais consecutivas, poderá ser descredenciada da ICP-Brasil.

9.11 Na ocorrência do descredenciamento mencionado no item 9.10, a entidade não poderá ter um novo pedido de credenciamento aceito pelo ITI pelo período mínimo de dois (2) anos.

……..…...” (NR)

Art. 5º O DOC-ICP-09, versão 3.3, passa a vigorar com as seguintes alterações:

“…….

1.1 Para os fins deste documento, entende-se como:

AÇÃO DE FISCALIZAÇÃO DE CERTIFICAÇÃO (AFC) – Procedimentos preparatórios, levantamento de informações, ações presenciais ou à distância, levantamento de evidências, pedidos complementação de informações através do documento

REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC) [1] e atividades do fiscal que devem estar relatadas no documento **RELATÓRIO DE FISCALIZAÇÃO (RF) [5]**.

a) **AUTORIDADE OUTORGANTE** – Autoridade competente e empossada no cargo de Diretor de Auditoria, Fiscalização e Normalização da AC Raiz, sendo, pela legislação, autorizado a praticar todos os atos necessários à realização do Procedimento de Fiscalização de Certificação (PFC) e que expede documentos relativos ao mesmo;

b) **AUTO DE INFRAÇÃO DE CERTIFICAÇÃO (AIC) [2]** – Documento preenchido pelo Fiscal da ICP-Brasil ao constatar infração por Prestador de Serviço de Certificação (PSCert) durante a fiscalização;

c) **FISCAL DA ICP-BRASIL** – Servidor lotado na Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz e no exercício das funções de fiscal, conforme indicado no documento **TERMO DE FISCALIZAÇÃO (TF) [3]**;

d) **FISCALIZAÇÃO** – Atividade de controle e inspeção sistemática, programada ou a qualquer tempo, do cumprimento das resoluções, normas, procedimentos e atividades dos Prestadores de Serviço de Certificação (PSCert) com a finalidade de examinar se as operações de cada um deles, isolada ou conjuntamente, se mantêm em conformidade com suas Declarações de Práticas, Políticas e com as Resoluções e normas gerais estabelecidas para as entidades integrantes da ICP-Brasil.

e) **INFRAÇÃO**

i Não atendimento a qualquer disposição legal da ICP-Brasil ou normas complementares estabelecidas pela AC Raiz;

ii Não-conformidade constatada a partir de fiscalização;

iii Obstrução, omissão ou má-fé por parte do PSCert tendente a prejudicar a ação fiscalizadora da AC Raiz;

f) **NOTIFICAÇÃO DA FISCALIZAÇÃO DE CERTIFICAÇÃO (NFC) [4]** - Documento pelo qual a Autoridade Outorgante dá ciência à Entidade Fiscalizada e a sua responsável hierárquica para que faça ou deixe de fazer alguma coisa;

g) **OBJETO DA FISCALIZAÇÃO** – Descrição do ponto de controle sob verificação. É um item das resoluções, um conjunto de itens, ou itens de resoluções associados;

h) **PRESTADOR DE SERVIÇO DE CERTIFICAÇÃO (PSCert)** – Qualquer entidade credenciada para operar na ICP-Brasil, como: as Autoridades Certificadoras (AC); as Autoridades de Registro (AR); as Autoridades de Carimbo do Tempo (ACT), os Prestadores de Serviço de Suporte (PSS), os Prestadores de Serviço Biométrico (PSBio), os Prestadores de Serviço de Confiança de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas (PSC); ou entidade vinculada, como o Laboratório de Ensaios e Auditoria (LEA) e outros que executem ou determinem a execução de itens de certificação presentes nas resoluções da ICP-Brasil;

i) **PROCEDIMENTO DE FISCALIZAÇÃO DE CERTIFICAÇÃO (PFC)** - Conjunto de ações que objetivam a verificação do cumprimento das normas, por parte das entidades credenciadas na ICP-Brasil, incluídos os atos administrativos de início e finalização e as ações de aplicação de penas, ampla defesa e comunicação de fiscalizações realizadas e dadas como conformes;

j) **PROCESSO ADMINISTRATIVO DE FISCALIZAÇÃO (PAF)** - Processo onde são arquivados todos os documentos e relatórios relativos ao Procedimento de Fiscalização de Certificação;

k) **RELATÓRIO DE FISCALIZAÇÃO (RF)** - Documento no qual o fiscal descreve o que constatou no Prestador de Serviço de Certificação, como foram as atividades e suas prescrições, subsidia o TFF e retrata todo a AFC, atividades executadas e constatações obtidas pelo Fiscal da ICP-Brasil;

l) **REQUISIÇÃO DE INFORMAÇÕES COMPLEMENTARES (RIC) [1]** - Documento no qual o fiscal ou auditor solicita informações complementares necessárias à condução do processo de fiscalização ou auditoria;

m) **TERMO DE FISCALIZAÇÃO (TF)** – Documento-base para a fiscalização e que indica a sua finalidade. Pode ser um **TERMO DE FISCALIZAÇÃO INICIAL (TFI), TERMO DE FISCALIZAÇÃO EXTENSIVO (TFE), TERMO DE FISCALIZAÇÃO COMPLEMENTAR (TFC) ou TERMO DE FISCALIZAÇÃO FINAL (TFF).**

……..” (NR)

Art. 6º O DOC-ICP-16, versão 1.0, passa a vigorar com as seguintes alterações:

“……..

4.7 Serviço de Gestão de Certificados de Atributos: trata-se de sistema de gestão do ciclo de vida de certificados de atributos regulado pela ICP-Brasil junto ao Prestador de Serviço de Confiança na modalidade de portal de assinaturas.

…….

6.1.5 Prestador de Serviço de Confiança – PSC da ICP-Brasil é uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais ou serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos.

…….

6.6 Módulo de Emissão e Guarda de Certificados de Atributo

A EEA deve manter repositório de certificados de atributo, sua LCR ou OCSP, quando aplicável.

A emissão e gestão do ciclo de vida do certificado de atributo da EEA poderá utilizar-se de serviço de assinatura e verificação de assinaturas digitais provido por PSC credenciado na ICP-Brasil.

…….…...” (NR)

Art. 7º Fica excluído o item 13.2.4 do DOC-ICP-02, versão 3.0, bem como os itens 6.3.4, 6.3.5 e 6.3.6 do DOC-ICP-08, versão 4.5.

Art. 8º Ficam aprovadas as seguintes versões dos documentos:

I - DOC-ICP-02 - POLÍTICA DE SEGURANÇA DA ICP-BRASIL– versão 3.1.

II - DOC-ICP-06 - POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL – versão 3.2.

III - DOC-ICP-08 - CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL – versão 4.6.

IV - DOC-ICP-09 - CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL – versão 3.4.

V - DOC-ICP-16 - VISÃO GERAL SOBRE CERTIFICADO DE ATRIBUTO PARA A ICP-

BRASIL – versão 1.1.

Parágrafo único. As demais cláusulas dos referidos documentos, nas suas versões imediatamente anteriores, em sua ordem originária, integram as presentes versões e mantêm-se válidas.

Art. 9º Ficam aprovadas novas versões dos seguintes documentos:

I - DOC-ICP-01 - DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL – versão 5.0, anexo I.

II - DOC-ICP-03 - CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL - versão 6.0, anexo II.

III - DOC-ICP-03.01 - CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL - versão 3.0, anexo III.

IV - DOC-ICP-04 - REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL - versão 7.0, anexo IV.

V - DOC-ICP-05 – REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL - versão 5.0, anexo V.

VI - DOC-ICP-05.02 - PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL - versão 2.0, anexo VI.

Parágrafo único. Os documentos referidos no caput substituem integralmente suas versões anteriores.

Art. 10. Os documentos alterados por esta resolução encontram-se disponibilizados, em sua totalidade, no sítio http://www.iti.gov.br.

Art. 11. Fica revogada a Instrução Normativa nº 07, de 15 de julho de 2016, que instituiu o documento REQUISITOS ADICIONAIS PARA ADERÊNCIA AOS PROGRAMAS DE RAÍZES CONFIÁVEIS DOS FORNECEDORES DE NAVEGADORES DE INTERNET – DOC-ICP-01.02.

Art. 12. Ficam extintas, no âmbito da ICP-Brasil, as Instalações Técnicas, Instalações Técnicas Secundárias, Postos Provisórios de Autoridades de Registro e os Prestadores de Serviço de Suporte de AR.

Parágrafo único. Os processos de credenciamento referidos no caput, em trâmite junto ao ITI, serão arquivados.

Art. 13. Ficam isentas da tarifa de prestação de serviço de emissão de certificados, de que trata o item 2, alínea 'b', do DOC-ICP-06, as AC que entrarem com pedido de emissão de certificados nas cadeias SSL e *Code Signing*, por motivo de adequação aos requisitos *WebTrust*, pelo prazo de até 180 (cento e oitenta) dias a contar da data da publicação desta Resolução.

Art. 14. As entidades da ICP-Brasil têm o prazo de até 120 (cento e vinte) dias, contados da data da publicação, para submissão à aprovação, pelo ITI, dos documentos afetos às mudanças previstas nesta Resolução.

§ 1º Quando se tratar de cadeias SSL e *Code Signing,* antes de submeter ao ITI, deve a Autoridade Certificadora ou mesmo o Prestador de Serviço de Suporte, sempre copiada a cadeia hierárquica, mediante solicitação eletrônica encaminhada por seu(s) representante(s),

requisitar, no endereço cgnpe@iti.gov.br, a geração do OID específico que será utilizado.

§ 2º Após a submissão ao ITI, da DPC e PC ajustadas, as AC estarão autorizadas a operar de acordo com as práticas declaradas de imediato, ainda que sem a aprovação expressa do ITI, sob a obrigação de correções/ajustes caso sejam apontadas após análise do ITI.

Art. 15. Para fins de auditoria, as mudanças previstas nesta Resolução devem ser observadas no ano civil subsequente ao da publicação desta Resolução.

Art. 16. As AR e as AC têm o prazo de até 120 (cento e vinte) dias, contados da data da publicação desta Resolução, para concluírem a transferência dos dossiês para o ambiente de AC.

Art. 17. Esta Resolução entra em vigor na data de sua publicação.

FERNANDO WANDSCHEER DE MOURA ALVES

Assinado de forma digital por FERNANDO WANDSCHEER DE MOURA ALVES
Dados: 2019.06.11 18:18:15 -03'00'

FERNANDO WANDSCHEER DE MOURA ALVES

Anexo I

Infraestrutura de Chaves Públicas Brasileira

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL

(DOC-ICP-01)

Versão 5.0

30 de maio de 2019

Infraestrutura de Chaves Públicas Brasileira

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
Resolução 151, de 30 de maio de 2019 (Versão 5.0)		Aprova a versão 5.0 do DOC-ICP-01.
Resolução 147, de 07 de novembro de 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 143, de 06 de setembro de 2018 (Versão 4.6)	7.1.2 e 7.1.4	Inclusão das cadeias V6, V7, V8 e V9.
Resolução 116, de 09 de dezembro de 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 104, de 23 de abril de 2015 (Versão 4.4)	7.1.2, item c) 7.1.4, item e)	Inclusão da cadeia V4
Resolução 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.
Resolução 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 81, de 17.06.2010 (versão 4.1)	7.1.2, 7.1.4, 7.2.4	Inclusão das cadeias V2 e V3
Resolução 50, de 19.11.2008	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 que aprovou alteração	*Item Alterado*	*Descrição da Alteração*
(versão 4.0)		
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
Resolução 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 38, de 18.04.2006 (versão 2.0)	Diversos	Criação do DOC-ICP-01 consolidando documentos anteriores

1 INTRODUÇÃO

1.1 Visão Geral

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.

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

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.

A AC Raiz possui os certificados de níveis mais altos na ICP-Brasil. Esses certificados contém as chaves públicas correspondente 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.

A estrutura desta DPC está baseada na RFC 3647.

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

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

Os procedimentos de aprovação da DPC da AC Raiz são estabelecidos a critério do CG da 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	Comitê Gestor
DN	*Distinguished Name*
DOU	Diário Oficial da União
DPC	Declaração de Práticas de Certificação
DPCT	Declaração de Práticas de Carimbo 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	Políticas 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

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.

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 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.

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

A AC Raiz comunicará, por escrito, qualquer alteração nesta DPC às AC 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

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. 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

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

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

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, atualizada pela RFC 6712, 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

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.

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

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

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

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].

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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

4.2.1 Execução das funções de identificação e autenticação

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

4.2.2 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.

4.2.3 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

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.

As chaves públicas dos certificados autoassinados são publicadas no DOU.

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

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.

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 parágrafo 2 do documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [4].

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.

A AC Raiz entrega o certificado emitido, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10], 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

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 Cerimônia de Emissão de Certificado, Termo de Cerimônia de Entrega de Chave Pública e 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:

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.

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

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:

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.

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.

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.

4.9.2 Quem pode solicitar revogação

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 deve processar o pedido de revogação

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

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.

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

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.

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:

1. Segurança física e controles ambientais;
2. Controles de integridade dos sistemas, incluindo gerenciamento de configuração, manutenção de integridade de código confiável e detecção e prevenção de incidentes;
3. Segurança de rede e gerenciamento de firewalls, incluindo restrições de porta e filtragem de endereços IP;
4. Gerenciamento de usuários, segregação de funções, capacitação, conscientização e treinamento; e
5. Controles de acesso lógico, com registro de atividades e de inatividade, a fim de fornecer responsabilidades individuais.

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

1. 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;

2. 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

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

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.

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.

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

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.

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.

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.

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:

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.

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.

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.

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.

Pessoas que não estejam envolvidas com essas atividades não deverão ter permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não poderão permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

No terceiro nível 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.

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.

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.

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.

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

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).

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

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

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.

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.

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

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.

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.

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.

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.

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

O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, 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

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.

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

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.

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.

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.

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.

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

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

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.

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.
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”) 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

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.

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:

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;

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;

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;

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;

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;

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:

a) Presidência do ITI;

b) Diretoria de Infraestrutura de Chaves Públicas do ITI;

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

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

e) Diretoria de Tecnologia da Presidência da República.

5.2.2 Número de pessoas necessário por tarefa

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.

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.

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

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.

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.

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

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.

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.

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.

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

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

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

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.

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.

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.

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

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.

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

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.

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

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.

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.

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.

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.

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

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.

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

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.

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

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

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.

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)

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.

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

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.

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

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

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

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.

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 Procedimentos de cópia de arquivo

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.

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

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.

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).

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

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.

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.

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

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.
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

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.

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

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.

Demais procedimentos estão descritos no PCN da AC Raiz.

5.7.4 Capacidade de continuidade de negócio após desastre

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.

O Plano de Recuperação de Desastres junto com o Plano de Continuidade dos Negócios, conforme descrito na Seção 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.

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, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

O par de chaves criptográficas da AC Raiz é gerado pela própria AC Raiz, em hardware específico, conforme o detalhado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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.

Os algoritmos e dispositivos criptográficos a serem utilizados para as chaves criptográficas da AC Raiz estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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 definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [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 Entrega de chave pública da AC Raiz às terceiras partes

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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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

Os parâmetros de geração de chaves assimétricas da AC Raiz adotam o padrão definido no documento PADRÕES E ALGORIOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

Os parâmetros são verificados de acordo com as normas referenciadas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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 no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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

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 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

Requisitos técnicos específicos de segurança computacional

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.

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).

6.5.1 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. O certificado da AC Raiz é o único certificado auto-assinado 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.

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

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

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 dessa 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.

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**: somente os bits keyCertSign e cRLSign devem estar ativados;

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

d.1) 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.

7.1.3 Identificadores de algoritmo

O certificado da AC Raiz é assinado com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

O certificado de AC de nível subsequente ao da AC Raiz é assinado com o uso de algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

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-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

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:

DN do titular:

C = BR

O = ICP-Brasil

OU = <CN da cadeia>

CN = <nome da AC subordinada>

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

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

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.

7.1.8 Sintaxe e semântica dos qualificadores de política

Os certificados emitidos pela AC Raiz implementa 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:

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

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

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.

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

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

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

Autorizações formais podem ser apresentadas de duas formas:

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

b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo

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

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:

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.

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.

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.

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].

Serviço

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

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*

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

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 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

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.

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.

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

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.

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.

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 da ICP-Brasil, prevalecerá sempre a última editada.

9.16.2 Cessão

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

9.16.3 Independência de disposições

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

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17 Outras provisões

Não se aplica.

10 DOCUMENTOS REFERENCIADOS

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

Ref.	*Nome do documento*	*Código*
[1]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[3]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[4]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06

[5]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[9]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08

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

Ref.	***Nome do documento***	***Código***
[10]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

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

Ref.	***Nome do documento***	***Código***
[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

Anexo II

Infraestrutura de Chaves Públicas Brasileira

CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL

DOC-ICP-03 - versão 6.0

30 de maio de 2019

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 151, de 30.05.2019 (Versão 6.0)	1, 2, 3 e 4	Simplificação dos processos da ICP-Brasil. Alteração dos critérios para credenciamento.
Resolução nº 144, Resolução nº 148 e Resolução nº 149, de 07.11.2018 (Versão 5.4)	2.2.3.3.3 e 3.2.3.1; Anexo II – 3.2; e Anexo I – 3.2	Estabelece novos requisitos para abertura de postos provisórios e atualiza e-mail para credenciamento simplificado. Critério para qualificação econômico-financeira de entidades sem fins lucrativos. Atualiza parâmetros para habilitação econômico-financeira e política tarifária.
Resolução nº 133 e Resolução nº 134, de 07.12.2017 (Versão 5.3)	3.2.2.2, 4.2.2.3, 4.4.2.3 3.2.3, 3.2.4, 5.3	Modifica os procedimentos de extinção de Instalação Técnica de AR e descredenciamento de AR e PSS. Modifica critérios para abertura e encerramento de Posto Provisório.
Resolução n° 132, de 10.11.2017 (Versão 5.2)	1, 2.1, 2.1.6, 2.2.7, 3.6, 4.5A, 4.6, 5.1, 5.2, 5.3 e Anexo VI	Institui o Prestador de Serviço de Confiança.
Resolução n° 130, de 19.09.2017 (Versão 5.1)	3.2.1.1, 3.2.1.2, 3.2.1.4, 3.2.1.5, 3.2.1.6 e 3.2.2.1	Atualização dos procedimentos para abertura de nova instalação técnica.
Resolução n° 125, de 13.09.2017 (Versão 5.0)	3.1.a, 3.1.d e 3.2.2.4	Incluir o PSBio nas previsões de manutenção de credenciamento. Unifica a definição de prazo para envio do relatório de auditoria. Ajuste na numeração do item 3.2.2.4.
Resolução n° 114, de 30.09.2015 (Versão 4.9)	1, 2.1, 2.1.4.1, 2.1.4.2, 2.2.1.6, 2.2.6, 3.5, 4.5, 4.6, 5.2, 5.3 e anexo V.	Cria o processo de credenciamento do PSBIO.
Resolução 108, de 25.08.2015 (Versão 4.8	2.2.1.8 e 2.2.1.9	Desconsideração da personalidade jurídica.

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução 102, de 29.04.2014 (Versão 4.7)	Item 3.2, alíneas "d" e "e"; insere item 3.2.1.4 e renumera os subsequentes.	Insere qualificação econômico-financeira para PSS de ACT e regulamenta processo simplificado para funcionamento de Inst. Técnica de AR já credenciada.
Resolução 88, de 25.05.2012 (Versão 4.6)	Item 3.1, alínea "a"	Inclui indício ou fraude comprovada no rol de fatos que devem obrigatoriamente ser comunicados à AC Raiz da ICP-Brasil.
Resolução 86, de 6.12.2011 (Versão 4.5)	Item 3 dos Anexos I, II, III e IV; Item 4 do Anexo II	Corrige omissão de exigência de certidão para qualificação econômico-financeiro. Retira exigência de minuta de Termo de titularidade.
Resolução 83, de 13.08.2010 (Versão 4.4)	Item 3 dos Anexos I, II, III e IV	Altera o item 3 dos anexos referenciados, incluindo novos requisitos para o credenciamento de entidades da ICP-Brasil e os respectivos valores de garantia
Resolução 74, de 24.11.2009 (Versão 4.3)	Item 4 Anexo II, alínea c	Inclusão de minuta de termo de titularidade
Resolução 70, de 18.11.2009 (Versão 4.2)	Itens 2.1.2, alínea "a", 2.2.1, 2.2.3.1.1, alínea "d", 2.2.3.2.1, alínea "d", 2.2.3.3.3, 3.2.3.3	Alteração dos itens relacionados
Resolução 67, de 09.06.2009 (Versão 4.1)	Itens 3.2.1.3, 3.2.5.3, 3.2.5.4	Alteração dos itens relacionados
Resolução 52, de 19.11.2008 (Versão 4.0)	1, 2.1.3, 2.1.4.1, 2.1.4.2, 2.2.1.5, 2.2.4, 2.2.5.1.2, 2.2.5.3, 3.3, 3.4, 4.3, 4.4.2.1, 4.4.2.2, Anexo IV	Inclusão de referências a Autoridades de Carimbo de Tempo
Resolução 47, de 23.11.2007 (versão 3.0)	2.1.2	Alterados os documentos a serem apresentados caso a instalação técnica de uma AR se localize em endereço diferente do de sua sede administrativa

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
	3.1.d	Alterada a data para apresentação do cronograma anual de auditoria das ACs para 15 de março
	3.2.1	Inclusão dos subitens 3.2.1.1 e 3.2.1.3 e renumeração dos demais
	Item 3.a dos Anexos I, II e III	Substituição da exigência de apresentação de balanço contábil por apresentação de parecer de contador com registro no CNAI
Resolução 40, de 18.04.2006 (Versão 2.0)	Diversos	Criação do DOC-ICP-03, consolidando documentos anteriores

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade Certificadora do Tempo
AR	Autoridades de Registro
CG	Comitê Gestor
Code Signing	Assinatura de Código
CPF	Cadastro de Pessoas Físicas
DPC	Declaração de Práticas de Certificação
DPCT	Declaração de Práticas de Certificação do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
PC	Políticas de Certificado
PCT	Política de Certificação do Tempo
PSBio	Prestador de Serviço Biométrico
PS	Política de Segurança
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
SSL/TLS	*Secure Socket Layer/Transport Layer Security*
TimeStamping	Carimbo do Tempo

1 INTRODUÇÃO

1.1 Este documento estabelece os critérios e procedimentos a serem observados para o credenciamento, manutenção do credenciamento e descredenciamento de Autoridades Certificadoras (ACs), de Autoridades de Registro (ARs), de Autoridades de Carimbo do Tempo (ACTs), de Prestadores de Serviço de Suporte (PSSs), de Prestadores de Serviço Biométrico (PSBios) e de Prestadores de Serviço de Confiança (PSC) de Assinatura Digital e Armazenamento de Chaves Criptográficas no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

1.2 Para o presente documento aplicam-se os seguintes conceitos:

a) Autoridade Certificadora - AC: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, expedir, distribuir, renovar, revogar e gerenciar certificados digitais.

b) Autoridade de Carimbo do Tempo – ACT: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir Carimbos do Tempo.

c) Autoridade de Registro - AR: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável pela interface entre o usuário e a Autoridade Certificadora - AC. É sempre vinculada a uma AC e tem por objetivo o recebimento, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes.

d) Prestadores de Serviço Biométrico - PSBios: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, com capacidade técnica para realizar a identificação e a verificação biométrica do requerente de um certificado digital em um ou mais bancos/sistemas de dados biométrico da ICP-Brasil, como estabelecido no DOC-ICP-05.03 [16].

e) Prestador de Serviço de Confiança - PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, que provê serviços de armazenamento de chaves privadas para usuários finais, ou serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos, nos termos do DOC-ICP-17 [17], cabendo à AC Raiz, por meio de Instrução Normativa, determinar os procedimentos técnicos para operação desses PSC.

f) Prestador de Serviço de Suporte - PSS: entidade credenciada, pública ou privada, subordinada à hierarquia da ICP-Brasil, utilizada pelos demais entes credenciados para prestação de serviços relacionados às suas respectivas atividades, e se classificam em três categorias, conforme o tipo de serviço prestado:

    a) disponibilização de infraestrutura física e lógica;

    b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

2 CREDENCIAMENTO

2.1 Critérios

Os candidatos ao credenciamento na ICP-Brasil devem atender aos seguintes critérios:

a) ser órgão ou entidade de direito público ou pessoa jurídica de direito privado;

b) estar quite com todas as obrigações tributárias e os encargos sociais instituídos por lei;

c) atender aos requisitos relativos à qualificação econômico-financeira estabelecidos, conforme a atividade a ser desenvolvida, nos anexos I, II, III, IV, V e VI; e

d) atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica ou contratual, constantes dos documentos relacionados nos Anexos I, II, IV, V e VI, aplicáveis aos serviços a serem prestados.

2.1.1 Critérios para credenciamento de AC

Os candidatos ao credenciamento como AC devem ainda:

a) apresentar, no mínimo, uma entidade operacionalmente vinculada, candidata ao credenciamento para desenvolver as atividades de AR, ou solicitar o seu próprio credenciamento como AR;

b) apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS;

c) ter sede administrativa localizada no território nacional; e

d) ter instalações operacionais e recursos de segurança física e lógica, inclusive sala-cofre, compatíveis com a atividade de certificação, localizadas no território nacional, ou contratar PSS que as possua.

2.1.2 Critérios para credenciamento de AR

Os candidatos ao credenciamento como AR devem ainda:

a) estar operacionalmente vinculados a, pelo menos, uma AC ou candidato a AC; e

b) ter sede administrativa em território nacional e recursos de segurança compatíveis com a atividade de registro, conforme disposto no DOC-ICP-03.01[18].

2.1.3 Critérios para credenciamento de ACT

Os candidatos ao credenciamento como ACT devem ainda:

a) apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS;

b) ter sede administrativa localizada no território nacional; e

c) ter instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de emissão de carimbos do tempo, localizadas no território nacional, ou contratar PSS que as possua.

2.1.4 Critérios para credenciamento de PSS

Os candidatos ao credenciamento como PSS devem ainda:

a) estar operacionalmente vinculados a, pelo menos, uma AC ou candidato a AC, ou uma ACT ou candidato a ACT, ou a um PSBio ou candidato a PSBio, ou um PSC ou candidato a PSC;

b) ter sede administrativa, instalações operacionais e recursos de segurança física e lógica compatíveis com as atividades a serem desempenhadas; e

c) ter instalações operacionais e recursos de segurança física e lógica compatíveis com o tipo de serviço prestado, localizados no território nacional.

2.1.5 Critérios para credenciamento de PSBio

Os candidatos ao credenciamento como PSBios devem ainda:

a) apresentar a relação de eventuais candidatos ao credenciamento para desenvolver as atividades de PSS;

b) ter sede administrativa localizada no território nacional; e

c) ter instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de identificação biométrica, conforme disposto no DOC-ICP-05.03[16], localizadas no território nacional, ou contratar PSS que as possua.

2.1.6 Critérios para credenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

Os candidatos ao credenciamento como PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas devem ainda:

a) ter sede administrativa localizada no território nacional; e

b) ter instalações operacionais e recursos de segurança física e lógica compatíveis com a atividade de armazenamento de chaves privadas para usuários finais ou realizar serviços de assinatura digital e verificação da assinatura digital ou ambos, conforme disposto no DOC-ICP-17 [17], localizadas em território nacional, ou contratar PSS que as possua.

2.2 Procedimentos

2.2.1 Diretrizes Gerais

2.2.1.1 O processo de credenciamento obedece a procedimentos específicos, relacionados com a natureza da atividade a ser desenvolvida no âmbito da ICP-Brasil.

2.2.1.2 O pedido inicial de credenciamento deverá ser encaminhado à AC Raiz por intermédio da cadeia de certificação à qual a candidata ao credenciamento se encontrar operacionalmente vinculada, iniciando-se a tramitação pela AC, ou candidato à AC de nível imediatamente superior à interessada e, a partir daí, respeitando-se a hierarquia da cadeia, até chegar à AC Raiz. As demais comunicações e requerimentos à AC Raiz, inclusive a complementação da documentação inicialmente encaminhada, poderão ser encaminhados diretamente à AC Raiz pela interessada.

2.2.1.3 As ACs serão responsáveis por comunicar as decisões do CG da ICP-Brasil ou da AC Raiz às entidades que lhes estejam operacionalmente vinculadas, respeitando a hierarquia de AC.

2.2.1.4 As ACTs e PSCs se comunicarão diretamente com a AC Raiz.

2.2.1.5 O deferimento do pedido de credenciamento será publicado no Diário Oficial da União e importará a autorização para funcionamento no âmbito da ICP-Brasil.

2.2.1.6 Em cada etapa da tramitação, a entidade que receber a solicitação de credenciamento de AC, AR, ACT ou PSBiotem prazo de até 30 (trinta) dias corridos para analisá-la e encaminhá-la à entidade de nível imediatamente superior, caso a solicitação seja acatada ou, se recusada, devolvê-la ao postulante com fundamentação da recusa.

2.2.1.7 Havendo recusa ou findo o prazo estabelecido no item 2.2.1.6, caberá recurso do postulante à AC Raiz.

2.2.1.8 Em caso de infração à lei ou abuso de direito, o ITI poderá, a qualquer tempo, mediante despacho fundamentado e assegurada a ampla defesa, desconsiderar a personalidade jurídica da interessada e obstar o seu credenciamento ou determinar o descredenciamento na ICP-Brasil.

2.2.1.9 Entende-se por desconsideração da personalidade jurídica a autorização, dada ao ITI, para impedir que pessoas jurídicas ou físicas que sejam sócias, administradoras ou representantes da empresa credenciada ou que solicita o credenciamento, retornem à ICP-Brasil em razão de descredenciamento decorrente de penalização anteriormente imposta.

2.2.2 Procedimentos para credenciamento de AC

2.2.2.1 Solicitação

2.2.2.1.1 As solicitações dos candidatos ao credenciamento como AC na ICP-Brasil serão encaminhadas à AC Raiz mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AC [1] devidamente preenchido e assinado pelo representante legal do candidato a AC;

b) documentos relacionados no Anexo I;

c) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2] devidamente preenchido e assinado pelos representantes legais dos candidatos a AC e AR;

d) documentos relacionados no Anexo II, exceto na hipótese de o candidato a AR ser o próprio candidato a AC;

e) comprovante do pagamento da tarifa estabelecida nas DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [5], no caso de a credenciada ser AC de nível imediatamente subsequente à AC Raiz; e

f) se for solicitado o credenciamento de PSS:

i. formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais dos candidatos a AC e a PSS;

ii. documentos relacionados no Anexo III; e

iii. documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções:

1. disponibilização de infraestrutura física e lógica;

2. disponibilização de recursos humanos especializados; ou

3. disponibilização de infraestrutura física e lógica de recursos humanos especializados.

2.2.2.1.2 a solicitação de credenciamento deve estar separada por propósito de uso de chave, quais sejam:

i. autenticação de servidor (SSL/TLS);

ii. assinatura de documentos e proteção de e-mail (S/MIME);

iii. assinatura de código (Code Signing); e

iv. assinatura de carimbo do tempo (TimeStamping).

2.2.2.1.3 Os órgãos e entidades da Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios, bem como suas autarquias e fundações públicas, estão dispensados do pagamento da tarifa prevista no item 2.2.2.1.1.

2.2.2.1.4 A solicitação de credenciamento será protocolada perante o Protocolo Geral da AC Raiz.

2.2.2.1.5 Caso a solicitação de credenciamento não contenha todos os documentos relacionados nos anexos I, II ou III, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.2.2 Auditoria Pré-operacional

2.2.2.2.1 Ao protocolar a solicitação de credenciamento, o candidato a AC deverá estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil relacionados à atividade de autoridade certificadora e pronto para ser auditado, conforme os critérios e procedimentos para a realização de auditoria nas entidades da ICP-Brasil dispostos no DOC-ICP-08 [8].

2.2.2.2.2 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata.

2.2.2.2.3 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos pelo item 2.1, a AC Raiz intimará a candidata para que os cumpra no

prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.2.2.4 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata, por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.2.2.5 Apresentado o relatório final de auditoria, a autoridade competente decidirá, no prazo de 30 (trinta) dias, acerca do pedido de credenciamento formulado pela solicitante.

2.2.2.2.6 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei 9.784, de 29 de janeiro de 1999.

2.2.2.3 Ato de credenciamento

2.2.2.3.1 O credenciamento limita-se às PCs indicadas no formulário referido na alínea "a" do item 2.2.2.1.1 e poderá não contemplar todas as PCs solicitadas.

2.2.2.3.2 O deferimento total ou parcial, ou o indeferimento do credenciamento, será fundamentado e comunicado ao candidato a AC. É considerado deferimento parcial aquele que não contemplar todas as PCs propostas pelo candidato a AC.

2.2.2.3.3 Após a notificação do deferimento, o requisitante deverá:

a) apresentar à Diretoria de Auditoria, Fiscalização e Normalização do ITI, no prazo máximo de 10 (dez) dias após a notificação do deferimento , 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, válido por, no mínimo, 1 (um) ano;

b) emitir o certificado da AC credenciada e de sua LCR, os quais devem ser apresentados à Diretoria de Auditoria, Fiscalização e Normalização do ITI, no prazo máximo de 10 (dez) dias após a notificação do deferimento, para análise de conformidade e posterior publicação no site do ITI.

2.2.2.3.4 Os órgãos e entidades da Administração Direta da União, dos Estados, dos Municípios e do Distrito Federal, bem como suas autarquias e fundações públicas estão dispensados da apresentação da apólice prevista no item anterior.

2.2.2.3.5 Uma vez comprovado o atendimento das providências descritas no item 2.2.2.3.3, o ato de credenciamento será publicado no Diário Oficial da União, momento em que o credenciamento restará consumado.

2.2.2.3.6 Os prazos a que se referem o item 2.2.2.3.3 poderão ser prorrogados, a critério da autoridade competente para o credenciamento, mediante pedido do candidato a AC, o qual deverá expor as razões e justificativas para o não cumprimento dos prazos assinalados.

2.2.2.3.7 Decorrido os prazos descritos no item 2.2.2.3.3, sem que tenha havido a prorrogação na forma do item anterior, ou findo este, o processo será arquivado, e o eventual pedido de credenciamento da mesma entidade deverá ser tratado como um novo pedido de credenciamento.

2.2.3 Procedimentos para credenciamento de AR:

2.2.3.1 Solicitação

2.2.3.1.1 As solicitações dos candidatos ao credenciamento como AR na ICP-Brasil serão encaminhadas à AC ou candidato a AC a que o candidato a AR esteja operacionalmente vinculado, por intermédio de formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2]. A AC ou candidato a AC que receber a solicitação deverá encaminhar para a AC Raiz os seguintes documentos:

a) o formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR [2], devidamente preenchido e assinado pelos representantes legais do candidato a AR e da AC ou do candidato a AC a que esteja operacionalmente vinculado;

b) documentos relacionados no Anexo II, exceto na hipótese de o candidato a AR ser a própria AC;

c) relatório final de auditoria pré-operacional da AR, realizada observando o disposto no item sobre fiscalização e auditoria de conformidade do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10]; ou declaração de que o referido relatório será encaminhado pela cadeia de AC para o endereço eletrônico auditoria@iti.gov.br, assinada digitalmente pelos responsáveis legais da AC.

2.2.3.1.2 A solicitação de credenciamento será protocolada perante o Protocolo Geral da AC Raiz.

2.2.3.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados no anexo II, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.3.2 Auditoria

2.2.3.2.1 A Diretoria de Auditoria, Fiscalização e Normalização examinará a documentação apresentada e poderá, caso julgue necessário, no prazo máximo de 30 (trinta) dias:

a) solicitar vista do material utilizado na auditoria (documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração do relatório);

b) exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata;

c) realizar auditoria pré-operacional por seu quadro próprio, elaborando relatório que prevalecerá sobre o apresentado pela candidata; ou

d) indeferir o pedido, caso não seja apresentado o relatório final de auditoria na forma descrita no item 2.2.3.1.1.

2.2.3.2.2 Com base no(s) relatório(s) finais de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento. Relatório final é aquele emitido quando a auditoria não detectar não-conformidades ou quando as não-conformidades apontadas em relatório preliminar já estiverem regularizadas e certificadas pela empresa que realizou o trabalho de auditoria.

2.2.3.2.3 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

2.2.3.3 Ato de credenciamento

2.2.3.3.1 O credenciamento do candidato a AR está condicionado ao credenciamento da AC a que está operacionalmente vinculado.

2.2.3.3.2 O deferimento ou o indeferimento do credenciamento será publicado no Diário Oficial da União.

2.2.3.3.3 Caso a AR já esteja credenciada na ICP-Brasil e deseje se vincular a qualquer outra AC também credenciada, deverá encaminhar correspondência ao Protocolo Geral da AC Raiz, assinada digitalmente pelos responsáveis legais da AC imediatamente subsequente à AC Raiz em cuja cadeia pretenda se vincular, informando o que se segue:

- a identificação das Autoridades Certificadoras a qual deseja se vincular;
- a data em que a AR iniciará as operações junto à AC a qual deseja se vincular; e
- qual o instrumento legal, a exemplo de contrato ou convênio, utilizado para descrever as responsabilidades desse vínculo entre as entidades envolvidas.

2.2.3.3.4 A vinculação da AR à nova cadeia será publicada na página eletrônica da AC Raiz.

2.2.4 Procedimentos para credenciamento de ACT

2.2.4.1 Solicitação

2.2.4.1.1 As solicitações dos candidatos ao credenciamento como ACT na ICP-Brasil serão encaminhadas à AC Raiz mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ACT [13] devidamente preenchido e assinado pelo representante legal do candidato a ACT;

b) documentos relacionados no Anexo IV;

c) comprovante do pagamento da tarifa estabelecida nas DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [5];

d) se for solicitado o credenciamento de PSS:

i. formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais dos candidatos a ACT e a PSS;

ii. documentos relacionados no Anexo III; e

iii. documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções:

1. disponibilização de infraestrutura física e lógica;
2. disponibilização de recursos humanos especializados; ou
3. disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

2.2.4.1.2 Os órgãos e entidades da Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios, bem como suas autarquias e fundações públicas, estão dispensados do pagamento da tarifa prevista no item anterior.

2.2.4.1.3 A solicitação de credenciamento será protocolada perante o Protocolo Geral da AC Raiz.

2.2.4.1.4 Caso a solicitação de credenciamento não contenha todos os documentos relacionados nos anexos III ou IV, quando for o caso, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, prorrogável por decisão da autoridade competente para o credenciamento, contados do recebimento de ofício enviado pela AC Raiz com aviso de recebimento pelo destinatário.

2.2.4.2 Auditoria Pré-operacional

2.2.4.2.1 Ao protocolar a solicitação de credenciamento, o candidato a ACT deverá estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil relacionados à atividade de autoridade certificadora do tempo e pronto para ser auditado, conforme os critérios e procedimentos para a realização de auditoria nas entidades da ICP-Brasil dispostos no DOC-ICP-08 [8].

2.2.4.2.2 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata.

2.2.4.2.3 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos, a AC Raiz intimará a candidata para que os cumpra no prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.4.2.4 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata, por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.4.2.5 Apresentado o relatório final de auditoria, a autoridade competente decidirá, no prazo de 30 (trinta) dias, acerca do pedido de credenciamento formulado pela solicitante.

2.2.4.2.6 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

2.2.4.3 Ato de credenciamento

2.2.4.3.1 O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado ao candidato a ACT.

2.2.4.3.2 Após a notificação do deferimento, o requisitante deverá:

a) apresentar à Diretoria de Auditoria, Fiscalização e Normalização do ITI, no prazo máximo de 10 (dez) dias após a notificação do deferimento, apólice de contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessa atividade, válido por, no mínimo, 1 (um) ano;

b) emitir os certificados para os equipamentos da ACT, por AC credenciada na ICP-Brasil, os quais devem ser apresentados à Diretoria de Auditoria, Fiscalização e Normalização do ITI, no prazo máximo de 10 (dez) dias após a notificação do deferimento, para análise de conformidade.

2.2.4.3.3 Os órgãos e entidades da Administração Direta da União, dos Estados, dos Municípios e do Distrito Federal, bem como suas autarquias e fundações públicas estão dispensados da apresentação da apólice prevista no item anterior.

2.2.4.3.4 Uma vez comprovado o atendimento das providências descritas no item 2.2.4.3.2, o ato de credenciamento será publicado no Diário Oficial da União, momento em que o credenciamento restará consumado.

2.2.4.3.5 Os prazos a que se referem o item 2.2.4.3.2 poderão ser prorrogados, a critério da autoridade competente para o credenciamento, mediante pedido do candidato a ACT, o qual deverá expor as razões e justificativas para o não cumprimento dos prazos assinalados.

2.2.4.3.6 Decorrido os prazos descritos no item 2.2.4.3.2, sem que tenha havido a prorrogação na forma do item anterior, ou findo este, o processo será arquivado, e o eventual pedido de credenciamento da mesma entidade deverá ser tratado como um novo pedido de credenciamento.

2.2.5 Procedimentos para credenciamento de PSS

2.2.5.1 Solicitação

2.2.5.1.1 As solicitações dos candidatos ao credenciamento como PSS na ICP-Brasil serão encaminhadas à AC, ACT ou PSC ou candidato a AC, ACT ou PSC a que o candidato a PSS esteja operacionalmente vinculado, diretamente ou por intermédio de PSBio ou de candidato a PSBio, por meio do formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3].

2.2.5.1.2 A AC, ACT ou PSC ou candidato a AC, ACT ou PSC que receber a solicitação deverá manter cópia sob sua guarda e encaminhar para a AC Raiz os seguintes documentos:

a) o formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS [3], devidamente preenchido e assinado pelos representantes legais da AC, ACT ou PSC ou candidato a AC, ACT ou PSC;

b) relatório final de auditoria pré-operacional do PSS, realizada observado o disposto no item sobre fiscalização e auditoria de conformidade do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10];

c) documentos relacionados no Anexo III; e

d) documento indicando as atividades específicas para as quais postula o credenciamento como PSS, selecionando uma dentre as seguintes opções:

1. disponibilização de infraestrutura física e lógica;
2. disponibilização de recursos humanos especializados; ou
3. disponibilização de infraestrutura física e lógica, e de recursos humanos especializados.

2.2.5.1.3 A solicitação de credenciamento será protocolada perante o Protocolo Geral da AC Raiz.

2.2.5.1.4 Caso a solicitação de credenciamento não contenha todos os documentos relacionados no anexo III, a AC Raiz determinará a intimação da candidata para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.5.2 Auditoria

2.2.5.2.1 A Diretoria de Auditoria, Fiscalização e Normalização examinará a documentação apresentada e poderá, caso julgue necessário:

a) solicitar vista do material utilizado na auditoria (documentos, registros históricos e demais elementos materiais que deram subsídios à elaboração do relatório);

b) exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata; ou

c) realizar auditoria pré-operacional por seu quadro próprio, elaborando relatório que terá prevalência sobre o apresentado pela candidata.

2.2.5.2.2 Com base no(s) relatório(s) de auditoria, a AC Raiz manifestar-se-á sobre o deferimento ou indeferimento da solicitação de credenciamento, em até 30 (trinta) dias, por meio de despacho fundamentado.

2.2.5.2.3 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

2.2.5.3 O credenciamento do candidato a PSS estará condicionado ao credenciamento da AC, ACT, PSC ou do PSBio a que esteja operacionalmente vinculado. O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado à AC, ACT ou PSC que deu encaminhamento ao requerimento.

2.2.6 Procedimentos para credenciamento de PSBio

2.2.6.1 Solicitação

2.2.6.1.1 As solicitações dos candidatos ao credenciamento como PSBio na ICP-Brasil serão encaminhadas ao ITI, por intermédio da cadeia hierárquica, mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PRESTADOR DE SERVIÇOS BIOMÉTRICOS, ADE-ICP-03.I [15], devidamente preenchido e assinado pelos representantes legais do candidato e da AC;

b) documentos relacionados no Anexo V;

c) identificação do local onde o PSBio realizará as suas operações e manterá seus equipamentos, documentação e materiais utilizados; e

d) identificação do serviço de diretório ou página web onde se obtêm o arquivo com a publicação da Política de Segurança - PS e a relação das autoridades certificadoras credenciadas na ICP Brasil atendidas pelos serviços biométricos os quais estão credenciado junto a ICP Brasil.

2.2.6.1.2 A solicitação de credenciamento será protocolada perante o Protocolo Geral da AC Raiz.

2.2.6.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados no Anexo V, o ITI determinará a intimação do candidato para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pelo ITI com comprovação de recebimento pelo destinatário.

2.2.6.2 Auditoria Pré-operacional

2.2.6.2.1 Ao protocolar a solicitação de credenciamento, o candidato a PSBIO deve estar em conformidade com todos os requisitos exigidos pelas resoluções do CG da ICP-Brasil relacionados à atividade de prestador de serviços biométricos e pronto para ser auditado, conforme os critérios e procedimentos para a realização de auditoria nas entidades da ICP-Brasil dispostos no DOC-ICP-08 [8].

2.2.6.2.2 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata.

2.2.6.2.3 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos pelo item 2.1, a AC Raiz intimará a candidata, via cadeia hierárquica, para que os cumpra no prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.6.2.4 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata, via cadeia hierárquica, por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.6.2.5 Apresentado o relatório final de auditoria, a autoridade competente decidirá, no prazo de 30 (trinta) dias, acerca do pedido de credenciamento formulado pela solicitante.

2.2.6.2.6 Sobre a decisão de indeferimento de solicitação de credenciamento caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

2.2.6.3 Ato de credenciamento

2.2.6.3.1 O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado, via cadeia hierárquica, ao PSBio que deu encaminhamento ao requerimento.

2.2.6.3.2 O ato de credenciamento será publicado no Diário Oficial da União, devendo o PSBio, por seu representante legal, apresentar termo de compromisso ao ITI, com a descrição de suas responsabilidades e o compromisso de desempenhar suas funções de acordo com padrões de idoneidade que asseguram a independência e neutralidade de suas avaliações bem como o devido rigor técnico e operacional.

2.2.6.3.3 O PSBio que já estiver credenciado na ICP-Brasil poderá prestar serviço a qualquer AC, a qual deverá comunicar ao ITI com 5 (cinco) dias de antecedência e publicar o fato em sua página web.

2.2.6.4 Vedações ao credenciamento

É vedada a contratação, subcontratação ou terceirização total ou parcial das atividades de cadastramento, atualização ou consulta para fins de verificação de dados biométricos do requerente pelos PSBio credenciados no âmbito da ICP Brasil, salvo a contratação de empresas fornecedoras de soluções biométricas, identificação (1:N) para um cadastro novo e verificação (1:1) em consultas on-line da biometria solicitada, desde que previamente solicitadas ao ITI, conforme Anexo V deste documento.

2.2.7 Procedimentos para credenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

2.2.7.1 Solicitação

2.2.7.1.1 As solicitações dos candidatos ao credenciamento como PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas na ICP-Brasil serão encaminhadas à AC Raiz, mediante a apresentação dos documentos a seguir relacionados:

a) formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PRESTADOR DE SERVIÇO DE CONFIANÇA DE ARMAZENAMENTO E ASSINATURA, ADE-ICP-03.K [4], devidamente preenchido e assinado pelos representantes legais do candidato;

b) documentos relacionados no Anexo VI;

c) identificação do(s) local(is) onde o candidato(s) realizará(ão) as suas operações e manterá(ão) seus equipamentos, documentação e materiais utilizados;

d) identificação do serviço de diretório ou página web onde se obtêm o arquivo com a publicação da Política de Segurança – PS.

2.2.7.1.2 A solicitação de credenciamento será protocolada perante o Protocolo Geral do AC Raiz.

2.2.7.1.3 Caso a solicitação de credenciamento não contenha todos os documentos relacionados no Anexo VI, o ITI determinará a intimação do candidato para que, sob pena de arquivamento do processo, supra as irregularidades no prazo máximo de 30 (trinta) dias, a contar do recebimento de ofício enviado pelo ITI com comprovação de recebimento pelo destinatário.

2.2.7.2 Auditoria Pré-Operacional

2.2.7.2.1 Ao protocolar a solicitação de credenciamento, o candidato a PSC deve estar em conformidade com todos os requisitos exigidos pelas resoluções do Comitê Gestor da ICP-Brasil relacionados à atividade de PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas e pronto para ser auditado, conforme os critérios e procedimentos para a realização de auditoria nas entidades da ICP-Brasil dispostos no DOC-ICP-08 [8].

2.2.7.2.2 Durante as diligências de auditoria a AC Raiz poderá exigir documentação adicional contendo especificações sobre equipamentos, produtos de hardware e software, procedimentos técnicos e operacionais adotados pela candidata.

2.2.7.2.3 Caso o relatório de auditoria aponte o não-cumprimento de quaisquer dos critérios para credenciamento exigidos pelo item 2.1, a AC Raiz intimará a candidata para que os cumpra no prazo que fixar, a contar do recebimento de ofício enviado pela AC Raiz com comprovação de recebimento pelo destinatário.

2.2.7.2.4 Após a comunicação da candidata de que atendeu os critérios de credenciamento apontados como não cumpridos no relatório de auditoria, a AC Raiz intimará a candidata por meio de ofício enviado com comprovação de recebimento pelo destinatário, determinando a realização de auditoria complementar, de modo a verificar as medidas adotadas.

2.2.7.2.5 Apresentado o relatório final de auditoria, a autoridade competente decidirá, no prazo de 30 (trinta) dias, acerca do pedido de credenciamento formulado pela solicitante.

2.2.7.2.6 Sobre a decisão de indeferimento de solicitação de credenciamento, caberá recurso administrativo da candidata à autoridade competente, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

2.2.7.3 Ato de credenciamento

2.2.7.3.1 O deferimento ou o indeferimento do credenciamento será fundamentado e comunicado ao candidato que deu encaminhamento ao requerimento.

2.2.7.3.2 O ato de credenciamento será publicado no Diário Oficial da União, devendo o candidato, por seu representante legal, apresentar termo de compromisso ao ITI, com a descrição de suas responsabilidades e o compromisso de desempenhar suas funções de acordo com padrões de idoneidade que asseguram a independência e neutralidade de suas avaliações bem como o devido rigor técnico e operacional.

2.2.7.3.3 O PSC de Armazenamento de Chaves Criptográficas que já estiver credenciado na ICP-Brasil poderá prestar serviço a qualquer usuário da ICP-Brasil, em parceria com uma AC, a qual deverá estar autorizada pelo ITI à prática de emissão declarada em sua PC/DPC, conforme disposto no subitem "b" do item 3.1.

2.2.7.4 Vedações ao credenciamento

É vedada a contratação, subcontratação ou terceirização total ou parcial das atividades de armazenamento das chaves privadas para usuários finais pelos PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas credenciados no âmbito da ICP-Brasil, salvo a contratação de empresas fornecedoras de soluções para hardwares criptográficos e sistemas para serviços de assinaturas digitais e verificação das assinaturas digitais, conforme Anexo VI deste documento.

3 MANUTENÇÃO DO CREDENCIAMENTO

As entidades credenciadas deverão manter atendidos os critérios definidos no item 2.1.

3.1 Manutenção de credenciamento de AC

A entidade credenciada para desenvolver as atividades de AC deverá:

a) comunicar, desde logo, à AC Raiz e à AC a que está subordinada:

i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;

ii. desvinculação de AC, de PSBio, de AR ou de PSSs credenciados;

iii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil cometida pelas ACs, ARs, PSSs. PSBios ou PSCs que lhe sejam operacionalmente vinculados; ou

iv. indício ou fraude comprovada na emissão de certificado por requerente que apresente documento ou informação falsa, no dia útil imediatamente subsequente à confirmação do ato, na forma estabelecida no ADE-ICP-03.H [14].

b) solicitar à AC Raiz autorização para alterar sua DPC, suas PCs ou sua Política de Segurança - PS, constantes dos documentos relacionados no Anexo I;

c) manter os titulares dos certificados informados acerca de eventual sucessão de AC ou AR operacionalmente vinculadas;

d) encaminhar à AC Raiz, dentro do prazo estabelecido no Plano Anual de Auditoria Operacional, definido no documento CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL, DOC-ICP-08 [8], cronograma das auditorias a serem realizadas, durante o ano, nas entidades que lhe sejam operacionalmente vinculadas;

e) encaminhar à AC Raiz relatórios de auditorias realizadas nas entidades que lhe sejam operacionalmente vinculadas, até 30 (trinta) dias após sua conclusão.

f) registrar alterações na sua infraestrutura de hardware, software ou procedimental relacionada diretamente com a atividade de AC, AR, PSS ou PSBio.

3.2 Manutenção de credenciamento de AR

3.2.1 A entidade credenciada para desenvolver as atividades de AR deverá:

a) comunicar, desde logo, à AC a que está operacionalmente vinculada:

i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;

ii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil por parte de seus funcionários;

b) observar a DPC, as PCs e a PS da AC a que estiver vinculada.

3.2.2 As serventias extrajudiciais autorizadas pelo Conselho Nacional de Justiça, nos termos do art. 236 da Constituição Federal, desde que formalmente vinculadas a uma AR já credenciada, poderão ter seus funcionários habilitados a atuar como agentes de registro.

3.3 Manutenção de credenciamento de ACT

A entidade credenciada para desenvolver as atividades de ACT deverá:

a) comunicar, desde logo, à AC Raiz:

i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;

ii. desvinculação de PSSs credenciados;

iii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil, cometida pelos PSSs que lhe sejam operacionalmente vinculados.

b) solicitar à AC Raiz autorização para alterar sua DPCT**,** suas PCTs ou sua Política de Segurança (PS), constantes dos documentos relacionados no Anexo IV;

c) encaminhar à AC Raiz relatórios de auditorias realizadas nas suas instalações técnicas, até 30 (trinta) dias após a conclusão das mesmas;

d) registrar alterações na sua infraestrutura de hardware, software ou procedimental relacionada diretamente com a atividade de AC, AR, PSS ou PSBio.

3.4 Manutenção de credenciamento de PSS

A entidade credenciada para desenvolver as atividades de PSS deverá:

a) comunicar à AC, ACT ou PSC ou candidato a AC, ACT ou PSC a que o candidato a PSS esteja operacionalmente vinculado, diretamente ou por intermédio de PSBio ou de candidato

a PSBio, qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;

b) observar a DPC, as PCs e a PS da AC, ou a DPCT, as PCTs e PS da ACT ou a DPPSC e PS do PSC a que estiver vinculada.

3.5 Manutenção de credenciamento de PSBio

A entidade credenciada para desenvolver as atividades de PSBio deverá, via cadeia hierárquica:

a) comunicar, desde logo, ao ITI:

i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores,

ii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil,

iii. qualquer alteração na sua Política de Segurança – PS.

b) encaminhar ao ITI relatórios de auditorias em até 30 (trinta) dias após a conclusão das mesmas;

c) observar o DOC-ICP-05.03 [16] e a PS aplicável; e

d) registrar alterações na sua infraestrutura de hardware, software ou procedimental relacionada diretamente com a atividade de AC, AR, PSS ou PSBio.

3.6 Manutenção de credenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

A entidade credenciada para desenvolver as atividades de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas deverá:

a) comunicar, desde logo, ao ITI:

i. qualquer alteração em seus atos constitutivos, estatuto, contrato social ou administradores;

ii. violação, de que tenha conhecimento, das diretrizes e normas técnicas da ICP-Brasil;

iii. qualquer alteração na sua Declaração de Práticas de Prestadores de Serviço de Confiança – DPPSC, Plano de Capacidade Operacional – PCO e Política de Segurança – PS.

b) encaminhar ao ITI relatórios de auditorias em até 30 (trinta) dias após a conclusão das mesmas;

c) observar o DOC-ICP-17.01 [9], a DPPSC, o PCO e PS aplicável; e

d) registrar alterações na sua infraestrutura de hardware, software ou procedimental relacionada diretamente com a atividade de AC, AR, PSS ou PSBio.

4 DESCREDENCIAMENTO

4.1 Descredenciamento de AC

4.1.1 Requisitos Gerais para o descredenciamento de AC

4.1.1.1 O descredenciamento de uma AC pode ocorrer em relação a todas as PCs para qual tenha sido credenciada ou em relação a PC específicas.

4.1.1.2 O descredenciamento de uma AC para todas as PCs credenciadas enseja a revogação do correspondente certificado e o descredenciamento de todas as entidades que lhe sejam operacionalmente vinculadas: AC subsequentes, AR ou PSS.

4.1.2 Hipóteses para o descredenciamento de AC

a) quando da expiração do prazo de validade de certificado da AC, sem que haja a emissão de novo certificado para substituí-lo;

b) quando do descredenciamento da AC de nível imediatamente superior;

c) quando do descredenciamento de AR única vinculada, sem que haja a solicitação de credenciamento de nova AR;

d) quando do descredenciamento de PSS único vinculado, que desempenhe atividades descritas nas DPCs e PCs da AC, de modo a inviabilizar a continuidade de operação da AC, sem que haja a solicitação de credenciamento de novo PSS e sem que a AC passe a desempenhar, ela própria, as atividades antes executadas pelo PSS;

e) a pedido da própria AC, mediante requerimento, em relação às suas atividades;

f) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.1.3 Procedimentos para descredenciamento de AC

4.1.3.1 Descredenciamento solicitado pela própria AC

Na hipótese de o descredenciamento ser solicitado pela própria AC, deverão ser obedecidos os seguintes procedimentos:

a) a AC comunicará, com 120 (cento e vinte) dias de antecedência, diretamente à AC Raiz e às entidades a ela vinculadas, e publicará em sua página *web*, para conhecimento dos titulares de certificados emitidos, a decisão de encerrar suas atividades de emissão de certificados no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCs especificadas; e

b) a AC divulgará, pelos 90 (noventa) dias imediatamente anteriores à expiração do certificado, em sua página *web*, a decisão de encerrar suas atividades no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCs especificadas.

4.1.3.2 Descredenciamento por determinação da AC Raiz

Na hipótese de descredenciamento da AC por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC o seu descredenciamento, com relação às PCs que especificar;

b) as ACs descredenciadas sob esta hipótese ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.1.3.3.a.

4.1.3.3 Descredenciamento por qualquer das hipóteses previstas

Em qualquer das hipóteses de descredenciamento de AC deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*

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.

4.2 Descredenciamento de AR

O descredenciamento de uma AR implicará a paralisação automática de suas operações.

4.2.1 Hipóteses para o descredenciamento de AR

São as seguintes as hipóteses para descredenciamento de AR:

a) quando do descredenciamento da AC a que esteja operacionalmente vinculada;

b) a pedido da AC à qual a AR esteja operacionalmente vinculada, mediante requerimento, em relação às atividades da AR;

c) a pedido da própria AR credenciada; ou

d) por determinação da AC Raiz, em razão do descumprimento dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.2.2 Procedimentos para descredenciamento de AR

4.2.2.1 Descredenciamento solicitado pela própria AC

4.2.2.1.1 Na hipótese de descredenciamento de AR a pedido da AC à qual a AR esteja operacionalmente vinculada, a AC enviará o respectivo requerimento à AC Raiz, informando:

a) o motivo do descredenciamento;

b) a data de encerramento das atividades da AR.

4.2.2.2 Descredenciamento por determinação da AC Raiz.

Na hipótese de descredenciamento da AR por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC e à AR o seu descredenciamento;

b) as ARs descredenciadas por determinação da AC Raiz ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.2.2.4.a;

c) nos casos de reincidência de descredenciamento por determinação da AC Raiz, as ARs descredenciadas ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 5 (cinco) anos, contados da data da publicação de que trata o item 4.2.2.4.a.

4.2.2.3 O pedido de descredenciamento por iniciativa da própria AR deverá ser feito por intermédio da AC a que se encontre vinculada, seguindo-se o procedimento descrito no item 4.2.2.1.

4.2.2.4 Em qualquer das hipóteses de descredenciamento de AR deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*

b) após a publicação referida na alínea anterior, a AC à qual a AR descredenciada estava operacionalmente vinculada deverá adotar os seguintes procedimentos, mantendo a guarda de toda a documentação comprobatória em seu poder:

i. revogar, em até 3 (três) dias úteis, no sistema de certificação, os acessos dos equipamentos de AR e as autorizações dos agentes de registro da AR descredenciada;

ii. inventariar os certificados emitidos pela AR no prazo máximo de 40 (quarenta) dias;

iii. transferir, se for o caso, de forma segura, a documentação dos certificados gerados pela AR descredenciada para o local identificado no requerimento de descredenciamento, no prazo máximo de 50 (cinquenta) dias;

iv. publicar, em sua página web, informação sobre o descredenciamento da AR, em até 5 (cinco) dias;

v. disponibilizar relatório descrevendo todos os procedimentos de descredenciamento adotados para avaliação pela auditoria operacional, no prazo máximo de 60 (sessenta) dias; e

vi. excluir agentes de registro do Cadastro de Agentes de Registro – CAR.

4.3 Descredenciamento de ACT

4.3.1 Requisitos Gerais para o descredenciamento de ACT

4.3.1.1 O descredenciamento de uma ACT pode ocorrer em relação a todas as PCTs para as quais tenha sido credenciada ou em relação a PCT específicas.

4.3.1.2 O descredenciamento de uma ACT para todas as PCTs credenciadas enseja a revogação dos correspondentes certificados e o descredenciamento de todos os PSSs que lhe sejam operacionalmente vinculados.

4.3.2 Hipóteses para o descredenciamento de ACT

a) a pedido da própria ACT, mediante requerimento, em relação às suas atividades;

b) quando do descredenciamento de PSS único vinculado, que desempenhe atividades descritas na DPCT e PCTs da ACTs, de modo a inviabilizar a continuidade de operação da ACT, sem que haja a solicitação de credenciamento de novo PSS e sem que a ACT passe a desempenhar, ela própria, as atividades antes executadas pelo PSS;

c) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.3.3 Procedimentos para descredenciamento de ACT

4.3.3.1 Descredenciamento solicitado pela própria ACT

Na hipótese de o descredenciamento ser solicitado pela própria ACT, deverão ser obedecidos os seguintes procedimentos:

a) a ACT comunicará, com 120 (cento e vinte) dias de antecedência, diretamente à AC Raiz e às entidades a ela vinculadas, e publicará em sua página *web*, para conhecimento dos subscritores, a decisão de encerrar suas atividades de emissão de carimbo do tempo no âmbito da ICP-Brasil ou de não mais emitir carimbos sob as PCTs especificadas; e

b) a ACT divulgará, pelos 90 (noventa) dias imediatamente anteriores ao encerramento, em sua página *web*, a decisão de encerrar suas atividades no âmbito da ICP-Brasil ou de não mais emitir certificados sob as PCTs especificadas.

4.3.3.2 Descredenciamento por determinação da AC Raiz

Na hipótese de descredenciamento da ACT por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à ACT o seu descredenciamento, com relação às PCTs que especificar;

b) as ACTs descredenciadas sob esta hipótese ficam impedidas de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.3.3.3.a.

4.3.3.3 Descredenciamento por qualquer das hipóteses previstas

Em qualquer das hipóteses de descredenciamento de ACT deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web;*

b) os PSSs operacionalmente vinculados deverão cessar, em relação às PCT objeto do descredenciamento, suas atividades de emissão de carimbos do tempo no âmbito da ICP-Brasil imediatamente após a comunicação de que trata a alínea anterior;

c) em caso de descredenciamento total de uma ACT:

i. a ACT ou a AC Raiz, conforme o caso, solicitará à AC emitente a revogação do(s) certificados(s) digital(is) do(s) equipamento(s) de carimbo do tempo da ACT descredenciada;

ii. a ACT que encerra as suas atividades transferirá os documentos e *logs* de auditoria gerados durante sua operação para outra ACT interessada ou, na falta dessa, à AC Raiz, para guarda pelo período estipulado nos regulamentos da ICP-Brasil.

4.4 Descredenciamento de PSS

4.4.1 Hipóteses para o descredenciamento de PSS

a) quando do descredenciamento da AC a que esteja operacionalmente vinculado;

b) a pedido da AC à qual esteja operacionalmente vinculado, mediante requerimento, em relação às atividades do PSS; ou

c) por determinação da AC Raiz em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento.

4.4.2 Procedimentos para descredenciamento de PSS

4.4.2.1 Descredenciamento solicitado pela própria AC ou ACT

Na hipótese de descredenciamento de PSS a pedido da AC ou ACT à qual o PSS esteja operacionalmente vinculado, a AC ou ACT enviará o respectivo requerimento à AC Raiz, informando:

a) o motivo do descredenciamento e

b) a data de encerramento das atividades do PSS.

4.4.2.2 Descredenciamento por determinação da AC Raiz.

Na hipótese de descredenciamento de PSS por determinação da AC Raiz, deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz comunicará à AC ou ACT e ao PSS o seu descredenciamento;

b) os PSSs descredenciados por determinação da AC Raiz ficam impedidos de apresentar novo pedido de credenciamento pelo prazo de 6 (seis) meses contados da publicação de que trata o item 4.4.2.3.a;

c) nos casos de reincidência de descredenciamento por determinação da AC Raiz, os PSSs descredenciados ficam impedidos de apresentar novo pedido de credenciamento pelo prazo de 5 anos, contados da data da publicação de que trata o item 4.4.2.3.a.

4.4.2.3 Descredenciamento por qualquer das hipóteses previstas

Em qualquer das hipóteses de descredenciamento de PSS deverão ser obedecidos os seguintes procedimentos:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web*;

b) após a publicação referida na alínea anterior, a AC à qual o PSS descredenciado estava operacionalmente vinculado deverá adotar os seguintes procedimentos, mantendo a guarda de toda a documentação comprobatória em seu poder:

i. publicar, em sua página *web*, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso, em até 5 (cinco) dias úteis; e

ii. disponibilizar relatório descrevendo todos os procedimentos de descredenciamento adotados para avaliação pela auditoria operacional, no prazo máximo de 60 (sessenta) dias.

4.5 Descredenciamento de PSBio

4.5.1 Hipóteses para o descredenciamento de PSBio

a) a pedido do próprio PSBio, mediante requerimento, em relação às suas atividades;

b) por determinação do ITI, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para

regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.5.2 Procedimentos para descredenciamento de PSBio

4.5.2.1 Descredenciamento solicitado pelo próprio PSBio

Na hipótese de o descredenciamento ser solicitado pelo próprio PSBio, o mesmo comunicará o fato, com 60 (sessenta) dias de antecedência, diretamente ao ITI e às Autoridades Certificadoras que o contrataram e publicará em sua página web a decisão de encerrar suas atividades de prestação de serviços biométricos no âmbito da ICP-Brasil.

4.5.2.2 Descredenciamento por determinação do ITI

Na hipótese de descredenciamento por determinação do ITI, o PSBio descredenciado ficará impedido de apresentar novo pedido de credenciamento pelo prazo de 24 (vinte quatro) meses contados da publicação de que trata o item 4.5.2.3.a.

4.5.2.3 Descredenciamento por quaisquer das hipóteses anteriormente previstas:

a) o ITI divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página web;

b) o PSBio deverá cessar suas atividades de prestação de serviços biométricos no âmbito da ICP-Brasil imediatamente após a publicação de que trata a alínea anterior;

c) os documentos e dados biométricos dos titulares de certificados digital ICP-Brasil utilizados durante o período de operação na ICP-Brasil deverão ser armazenadas por outro PSBio credenciado, após aprovação do ITI;

d) quando houver mais de um PSBio interessado, assumirá a responsabilidade do armazenamento aquele indicado pela AC.

4.5.2.4 Da Responsabilidade.

a) a AC responderá solidariamente com o PSBio por qualquer dano oriundo de falha na prestação do serviço;

b) o PSBio, ainda que descredenciado, não poderá, sob pena de responsabilidade civil, criminal e administrativa, ceder, a qualquer título, os dados biométricos armazenados no desempenho de suas atividades na ICP-Brasil, à exceção do previsto na alínea “c” do item 4.5.2.3.

4.6 Descredenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

4.6.1 Hipóteses para o descredenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

a) a pedido do próprio PSC, mediante requerimento, em relação às suas atividades;

b) por determinação da AC Raiz, em razão de descumprimento de qualquer dos critérios e procedimentos exigidos para o seu funcionamento, após o decurso do prazo para

regularização, sem que a entidade tenha sanado a irregularidade e mediante processo administrativo.

4.6.2 Procedimentos para descredenciamento de PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas

4.6.2.1 Descredenciamento solicitado pelo próprio PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas.

Na hipótese de o descredenciamento ser solicitado pelo próprio PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas, o mesmo comunicará o fato, com 120 (cento vinte dias) dias de antecedência, diretamente à AC Raiz, aos titulares dos certificados e, se for o caso, às Autoridades Certificadoras, no caso de armazenamento de chaves privadas dos usuários finais, que o contrataram e publicará em sua página *web*, para conhecimento dos titulares dos certificados, a decisão de encerrar suas atividades de prestação de serviço de confiança no âmbito da ICP-Brasil, continuando a prestar os serviços regularmente nesse período.

4.6.2.2 Descredenciamento por determinação da AC Raiz.

Na hipótese de descredenciamento por determinação da AC Raiz, o PSC de Assinatura Digital e Armazenamento de Chaves Criptográficas descredenciado ficará impedido de apresentar novo pedido de credenciamento pelo prazo de 24 (vinte quatro) meses contados da publicação de que trata o item 4.6.2.3.a.

4.6.2.3 Descredenciamento por quaisquer das hipóteses anteriormente previstas:

a) a AC Raiz divulgará o fato, logo após a consumação da respectiva hipótese, no Diário Oficial da União e em sua página *web*;

b) os PSC deverão cessar suas atividades de armazenamento de novas chaves e/ou certificados digitais ou serviços de assinaturas ou ambos no âmbito da ICP-Brasil imediatamente após a publicação de que trata a alínea anterior;

c) as operações do PSC utilizados durante o período de operação na ICP-Brasil deverão ser realizadas por outro PSC credenciado, após aprovação da AC Raíz, que deverão entrar em contato com os titulares das chaves privadas para os novos procedimentos de uso;

d) os PSC descredenciados deverão imediatamente prover acesso aos HSMs e sistemas para outro PSC credenciado;

e) quando houver mais de um PSC interessado, assumirá a responsabilidade aquele indicado pelo PSC que encerra suas atividades;

f) em caso de não vinculação do PSC descredenciado a uma AC e não haja interessados em assumir as operações do PSC, os usuários deverão entrar em contato com a AC emissora para procedimentos de reemissão do seu par de chaves e respectivo certificado;

g) em caso de vinculação do PSC descredenciado a uma AC e não haja interessados em assumir as operações do PSC, as ACs que emitiram o par de chaves e o respectivo certificado deverão entrar em contato com os usuários para informações de uso ou reemissão do par de chaves e respectivo certificado.

4.6.2.4 Da Responsabilidade

a) o PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas, ainda que descredenciado, não poderá, sob pena de responsabilidade civil, criminal e administrativa, ceder, a qualquer título, as chaves privadas, certificados digitais e documentos armazenados no desempenho de suas atividades na ICP-Brasil, à exceção do previsto na alínea "c" do item 4.5.2.3.

4.7 Obrigações Subsistentes

As AC, as AR, os PSS, as ACT, os PSBio e os PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas operacionalmente vinculados têm o dever de observar as diretrizes e normas técnicas da ICP-Brasil, inclusive as obrigações que subsistirem após o encerramento das atividades de emissão e armazenamento de chaves privadas.

O ITI poderá determinar a revogação imediata do certificado digital emitido em desconformidade com as normas que regem a ICP-Brasil, com ônus à entidade infratora para ressalvar o direito de terceiros de boa-fé.

5 DOCUMENTOS REFERENCIADOS

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

Ref.	*Nome do documento*	*Código*
[10]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[11]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[12]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[17]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17
[5]	DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[6]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DE TEMPO DA ICP- BRASIL	DOC-ICP-12
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-13
[8]	CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08

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

Ref.	*Nome do documento*	*Código*
[9]	PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	DOC-ICP-17.01
[16]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03

[18]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01

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

Ref.	*Nome do documento*	*Código*
[1]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AC	ADE-ICP-03.A
[2]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE AR	ADE-ICP-03.B
[3]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PSS	ADE-ICP-03.C
[4]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PRESTADOR DE SERVIÇO DE CONFIANÇA DE ARMAZENAMENTO E ASSINATURA	ADE-ICP-03.K
[13]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE ACT	ADE-ICP-03.G
[14]	Modelo de COMUNICAÇÃO DE INDÍCIO OU FRAUDE NA EMISSÃO DE CERTIFICADO DIGITAL ICP-BRASIL	ADE-ICP-03.H
[15]	Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE PRESTADOR DE SERVIÇOS BIOMÉTRICOS	ADE-ICP-03.I

ANEXO I - DOCUMENTOS PARA CREDENCIAMENTO DE AC

O candidato a desenvolver as atividades de AC deve entregar à AC Raiz os seguintes documentos atualizados:

1 Relativos a sua habilitação jurídica:

a) ato constitutivo, devidamente registrado no órgão competente; e

b) documentos da eleição de seus administradores, quando aplicável;

2 Relativos a sua regularidade fiscal:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d” os órgão e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal)

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI)[1], ou, alternativamente, atendimento ao seguinte:

a) balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios; acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte;

1 Cadastro Nacional de Auditores Independentes (CNAI) regulamentado pela Resolução do CFC-Conselho Federal de Contabilidade, nº 1.019, de 18.02.2005.

b) será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;

LL = Lucro Líquido do exercício;

PL = (patrimônio líquido inicial + patrimônio líquido final)/2;

TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos (lucros e prejuízos obtidos) em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP média anual divulgada para o mesmo período a que se referir a média do patrimônio líquido;

d) caso o resultado obtido na alínea “b” ou “c” seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta Resolução, que possui PL igual ou superior a:

i. R$ 5.000.000,00: para AC de 1º nível;

ii. R$ 2.000.000,00: para AC de 2º nível;

e) caso a empresa tenha sido criada a menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, e esteja se candidatando a:

i. AC de 1º nível: além de possuir um patrimônio líquido de R$ 5.000.000,00, deverá apresentar fiança bancária no valor de seu capital social integralizado;

ii. AC subsequente: além de possuir um patrimônio líquido de R$ 2.000.000,00, deverá apresentar fiança bancária no valor de seu capital social integralizado.

f) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a inatividade, bem como deverá atender ao requisito previsto na alínea “e”.

4 Relativos a sua qualificação técnica:

a) Declaração de Práticas de Certificação - DPC, atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10];

b) Políticas de Certificado (PC), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [11];

c) Política de Segurança - PS, atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[12]; e

d) documento indicando se pretende emitir certificados para AC de nível imediatamente subsequente ao seu e, nesse caso, incluir os critérios e procedimentos de auditoria que pretende adotar em relação a essas ACs.

NOTA 1: Na hipótese de o candidato já estar credenciado como AC em relação a outra PC, o documento a apresentar fica restrito àquele descrito no item 4, alínea "b". Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AC ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo;

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

NOTA 4: As ACs que estiverem se credenciando com o objetivo de emitir certificados exclusivamente para AC subsequentes ficam dispensadas da apresentação de PC, devendo, todavia, a DPC incorporar todas as informações que deveriam constar na PC.

ANEXO II - DOCUMENTOS PARA CREDENCIAMENTO DE AR

O candidato a desenvolver as atividades de AR deve entregar à AC Raiz, por intermédio da AC ou candidato a AC a que esteja operacionalmente vinculado, os seguintes documentos atualizados:

1 Relativos a sua habilitação jurídica:

a) ato constitutivo, devidamente registrado no órgão competente; e

b) documentos da eleição de seus administradores, quando aplicável.

2 Relativos a sua regularidade fiscal:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d”, relativos a sua regularidade fiscal, os órgãos e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal):

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI)[2], ou, alternativamente, atendimento ao seguinte:

a) balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios; acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte;

2 Cadastro Nacional de Auditores Independentes (CNAI) regulamentado pela Resolução do CFC-Conselho Federal de Contabilidade, nº 1.019, de 18.02.2005.

b) será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;

LL = Lucro Líquido do exercício;

PL = (patrimônio líquido inicial + patrimônio líquido final)/2;

TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP divulgada para o mesmo período a que se referir a média do patrimônio líquido;

d) caso o resultado obtido na alínea “b” ou “c” seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta resolução, que possui PL igual ou superior a R$ 200.000,00;

e) caso a empresa tenha sido criada a menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, e esteja se candidatando a AR deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 200.000,00, com cobertura suficiente e compatível com as atividades a serem desempenhadas, válido por, no mínimo, 1 (um) ano, contado da data do protocolo do pedido de credenciamento.

f) caso o candidato seja uma entidade sem fins lucrativos, nos termos da legislação vigente, constituída há mais de dez anos, deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 200.000,00 (duzentos mil reais).

g) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a

inatividade, bem como deverá atender ao requisito previsto na alínea “e”.

4 Relativos aos contratos:

a) minuta do contrato ou do convênio com a AC a que está operacionalmente vinculada;

b) minuta do contrato ou do convênio com o PSS operacionalmente vinculado, se for o caso.

NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como AR em relação a outra PC, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AR ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo;

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO III - DOCUMENTOS PARA CREDENCIAMENTO DE PSS

O candidato a desenvolver as atividades de PSS deve entregar à AC Raiz, por intermédio da AC ou candidato a AC a que esteja operacionalmente vinculado, os seguintes documentos atualizados:

1 Relativos a sua habilitação jurídica:

a)ato constitutivo, devidamente registrado no órgão competente; e

b)documentos da eleição de seus administradores, quando aplicável.

2 Relativos a sua regularidade fiscal:

a)prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b)prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c)prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d)prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d”, relativos a sua regularidade fiscal, os órgãos e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal):

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI)[3], ou, alternativamente, atendimento ao seguinte:

a) balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios; acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte;

3 Cadastro Nacional de Auditores Independentes (CNAI) regulamentado pela Resolução do CFC-Conselho Federal de Contabilidade, nº 1.019, de 18.02.2005.

b) será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) resultado igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;

LL = Lucro Líquido do exercício;

PL = (patrimônio líquido inicial + patrimônio líquido final)/2;

TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP divulgada para o mesmo período a que se referir a média do patrimônio líquido;

d) caso o resultado obtido na alínea “b” ou “c” seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta resolução, que possui PL igual ou superior a:

i. R$ 5.000.000,00: para PSS de AC de 1º nível, dos tipos 1 ou 3;

ii. R$ 2.000.000,00: para PSS do tipo 2 para AC de qualquer nível e PSC;

iii. R$ 1.000.000,00: para PSS de ACT e de PSBio.

e) caso a empresa tenha sido criada a menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, e esteja se candidatando a:

i. PSS dos tipos 1 e 3 de AC de 1º nível: além de possuir um patrimônio líquido de R$ 5.000.000,00, deverá apresentar fiança bancária no valor de seu capital social integralizado;

ii. PSS do tipo 2 de AC de qualquer nível e do tipo 1 e 3 de AC subsequente: além de possuir um patrimônio líquido de R$ 2.000.000,00, deverá apresentar fiança bancária

no valor de seu capital social integralizado;

iii. PSS de PSC ou PSS de ACT deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 200.000,00, com cobertura suficiente e compatível com as atividades a serem desempenhadas, válido por, no mínimo, 1 (um) ano, contado da data do protocolo do pedido de credenciamento.

f) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a inatividade, bem como deverá atender ao requisito previsto na alínea "e".

NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como PSS em relação a outra PC, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a PSS ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo;

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO IV - DOCUMENTOS PARA CREDENCIAMENTO DE ACT

O candidato a desenvolver as atividades de ACT deve entregar à AC Raiz os seguintes documentos atualizados:

1 Relativos a sua habilitação jurídica:

a) ato constitutivo, devidamente registrado no órgão competente; e

b) documentos da eleição de seus administradores, quando aplicável;

2 Relativos a sua regularidade fiscal:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d)prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d”, relativos a sua regularidade fiscal, os órgãos e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal):

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI)[4], ou, alternativamente, atendimento ao seguinte:

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios; acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte.

4 Cadastro Nacional de Auditores Independentes (CNAI) regulamentado pela Resolução do CFC-Conselho Federal de Contabilidade, nº 1.019, de 18.02.2005.

b) Será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;

LL = Lucro Líquido do exercício;

PL = (patrimônio líquido inicial + patrimônio líquido final)/2;

TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) Caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP divulgada para o mesmo período a que se referir a média do patrimônio líquido.

d) Caso o resultado obtido na alínea “b” ou “c” seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta resolução, que possui PL igual ou superior a R$ 1.000.000,00.

e) Caso a empresa tenha sido criada a menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 1.000.000,00.

f) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a inatividade, bem como deverá atender ao requisito previsto na alínea “e”.

4 Relativos a sua qualificação técnica:

a) Declaração de Práticas de Carimbo do Tempo (DPCT), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE

PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP- BRASIL [6];

b) Políticas de Carimbo do Tempo (PCT), atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [7]; e

c) Política de Segurança (PS), atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[12].

NOTA 1: Na hipótese de o candidato já estar credenciado como ACT em relação a outra PCT, o documento a apresentar fica restrito àquele descrito no item 4, alínea "b". Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a ACT ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

b) ato constitutivo;

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

NOTA 3: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores (SICAF), registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO V - DOCUMENTOS PARA CREDENCIAMENTO DE PRESTADOR DE SERVIÇOS BIOMÉTRICOS - PSBio

O candidato a desenvolver as atividades de PSBio deve entregar ao ITI os seguintes documentos atualizados, por intermédio da cadeia hierárquica da AC ou candidata a AC à qual pretende se vincular:

1 Relativos a sua habilitação jurídica:

a) Ato constitutivo, devidamente registrado no órgão competente; e

b) Documentos da eleição de seus administradores, quando aplicável;

2 Relativos a sua regularidade fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d”, relativos a sua regularidade fiscal, os órgãos e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal):

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI)1, atestando a boa situação econômico-financeira do candidato ou, alternativamente, atendimento ao seguinte:

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte;

b) Será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;
LL = Lucro Líquido do exercício;
PL = (patrimônio líquido inicial + patrimônio líquido final)/2;
TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) Caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP divulgada para o mesmo período a que se referir a média do patrimônio líquido;

d) Caso o resultado obtido na alínea “b” ou “c” seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta resolução, que possui PL igual ou superior a R$ 2.000.000,00;

e) Caso a empresa tenha sido criada há menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 2.000.000,00.

f) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a inatividade, bem como deverá atender ao requisito previsto na alínea “e”.

4 Relativos a sua qualificação técnica:

a) Declaração de que assinará, após o credenciamento, Termo de Confidencialidade, sob o compromisso de obedecer as normas e políticas de segurança do ITI.

b) Política de Segurança (PS), atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[12].

NOTA: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

ANEXO VI - DOCUMENTOS PARA CREDENCIAMENTO DE PRESTADOR DE SERVIÇO DE CONFIANÇA DE ASSINATURA DIGITAL E ARMAZENAMENTO DE CHAVES CRIPTOGRÁFICAS

O candidato a desenvolver as atividades de PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas deve entregar a AC Raiz os seguintes documentos atualizados:

1 Relativos a sua habilitação jurídica:

a) Ato constitutivo, devidamente registrado no órgão competente; e

b) Documentos da eleição de seus administradores, quando aplicável;

2 Relativos a sua regularidade fiscal:

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do candidato, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade junto à Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) Prova de regularidade do candidato junto à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço – FGTS, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.

2.1 Ficam dispensados da apresentação dos documentos citados nas alíneas “c” e “d”, relativos a sua regularidade fiscal, os órgãos e entidades da administração direta, suas autarquias e fundações públicas.

3 Relativos a sua qualificação econômico-financeira (exceto entidades da administração pública direta e indireta, nas esferas federal, estadual e municipal):

3.1 Certidão negativa de falência ou recuperação judicial/extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio do requerente;

3.2 Parecer de Contador que possua certidão emitida pelo Cadastro Nacional de Auditores Independentes (CNAI), atestando a boa situação econômico-financeira do candidato ou, alternativamente, atendimento ao seguinte:

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, acompanhados de planilha evidenciando os cálculos previstos na alínea seguinte;

b) Será considerada em boa situação econômico-financeira o candidato que demonstrar, no exercício referido nas demonstrações financeiras, possuir RSPL (retorno sobre o patrimônio líquido) igual ou superior à TJLP média (Taxa de Juros de Longo Prazo, aprovada pelo Conselho Monetário Nacional, divulgada pelo Banco Central do Brasil com o código 256) a ser calculado da seguinte maneira:

$$RSPL = \frac{LL}{PL} \times 100 \geqslant TJLP$$

Onde:

RSPL = Retorno Sobre o Patrimônio Líquido;
LL = Lucro Líquido do exercício;
PL = (patrimônio líquido inicial + patrimônio líquido final)/2; TJLP = média das taxas a.a. divulgadas pelo BACEN no código 256 para o exercício.

c) Caso o candidato tenha obtido prejuízo no último exercício social exigível, poderá ser efetuado cálculo da média dos cinco últimos exercícios exigíveis. Para tanto será apurada a média aritmética do patrimônio líquido dos cinco últimos balanços, exigíveis pela legislação vigente, e a respectiva média aritmética dos resultados obtidos em cada balanço patrimonial considerado na apuração da média do PL. Neste caso, a comparação será realizada com a menor TJLP divulgada para o mesmo período a que se referir a média do patrimônio líquido;

d) Caso o resultado obtido na alínea "b" ou "c" seja menor que a TJLP, mas for maior que zero, o candidato deverá comprovar, com base nos documentos exigidos nesta resolução, que possui PL igual ou superior a R$ 2.000.000,00;

e) Caso a empresa tenha sido criada há menos de um ano e não seja exigível, nos termos da legislação vigente, a apresentação de balanço patrimonial e demonstração contábil do último exercício, deverá apresentar apólice de contrato de seguro de responsabilidade civil e operacional no valor mínimo de R$ 2.000.000,00;

f) caso a empresa tenha sido criada a mais de um ano, porém tenha ficado inativa no período da apresentação do balanço patrimonial e demonstrações contábeis do último exercício social, deverá apresentar Declaração de Informações Socioeconômicas e Fiscais (DEFIS) ou Declaração de Créditos Tributários e Débitos Federais (DCTF), encaminhada à Receita Federal, comprovando a inatividade, bem como deverá atender ao requisito previsto na alínea "e".

4 Relativos a sua qualificação técnica:

a) Declaração de que assinará, após o credenciamento, Termo de Confidencialidade, sob o compromisso de obedecer as normas e políticas de segurança do ITI.

b) Declaração de Prática de Prestador de Serviço de Confiança – DPPSC, atendendo às condições mínimas estabelecidas pelo documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE

PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL, DOC-ICP-17 [17];

c) Política de Segurança (PS), atendendo às condições mínimas estabelecidas na POLÍTICA DE SEGURANÇA DA ICP-BRASIL, DOC-ICP-02 [12];

d) Requisitos operacionais do PSC de Assinatura Digital e/ou Armazenamento de Chaves Criptográficas, atendendo às condições mínimas estabelecidas no documento PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL , DOC-ICP-17.01 [9];

e) Plano de Capacidade Operacional – PCO.

NOTA: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins do disposto no item 2, apresentar seu extrato.

Anexo III

Infraestrutura de Chaves Públicas Brasileira

CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL

DOC-ICP-03.01 - Versão 3.0

30 de maio de 2019

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 151, de 30.05.2019 Versão 3.0	1, 2, 3, 4, 5, 6, 7, 8 e 9	Simplificação dos Processos da ICP-Brasil.
Instrução Normativa nº 11, de 19.09.2018 Versão 2.6	4.1.2 e 4.1.7	Ampliação da obrigação de uso de georreferenciamento para todas as estações de trabalho das Autoridades de Registro.
Resolução 139 de 03.07.2018 Versão 2.5	6.2.3, 6.2.12	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
Instrução Normativa nº 05, de 06.04.2018 Versão 2.4	4.2.1	Formato para citação da coordenada geográfica.
Resolução n° 136, de 08.03.2018 Versão 2.3	1.3 e 9.1	Procedimentos para criação do termo de titularidade digital.
Resolução n° 130, de 19.09.2017 Versão 2.2	1.3, 1.6, 2.1.3, 2.2.3, 3.8, 4.1.2, 4.1.6, 4.2.1.”h”, 6.1.7.1, 6.1.7.2, 6.2.1 e 8A (novo)	Instituição da Instalação Técnica Secundária e a definição de procedimentos adicionais para validação externa.
IN 09/2015, de 07.12.2015 Versão 2.1	4.1.2.”k”	Incluída a referência da FCT ICP-BR para sincronização das estações de trabalho das ARs - item 4.1.2.”k”.
Resolução n° 115, de 11.11.2015 Versão 2.0	6.2.3 e 6.2.12	Criação de Política de Certificado A CF-e-SAT.
Resolução 90/2012, de 05.07.2012 Versão 1.6	7.2, 7.3	Altera o item 7.2 e inclui o item 7.3. que recomenda que em caso de apresentação da CNH - Carteira Nacional de Habilitação a AR consulte à base de dados dos órgãos emissores.
IN 05/2012, de 25.05.2012 Versão 1.5	7.2	Incluído item 7.2 que recomenda a convalidação de dados, quando apresentado a Cédula de Identidade para efeito de identificação de indivíduo.
IN 09/2010, de	2.2.4, 4.2.1, 6.1.7	Alteração dos itens citados para adequação ao

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
18.11.2010 Versão 1.4		processo de emissão de certificados digitais que integram o documento de Registro de Identidade Civil – RIC.
Resolução 74, de 24.11.2008 Versão 1.3	Os itens 1.3, alínea f, h e item 6.2.10	Alteração dos itens citados
IN 02/2008, de 06.08.2008 Versão 1.2	4.2.1.d	Alterado o requisito de timeout.
Resolução 10, de 15.09.2006 Versão 1.1	-	Estabelece diretrizes da política tarifária da AC Raiz.
Resolução 07, de 19.05.2006 Versão 1.0	-	Aprovar a versão 1.0 do documento

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AGR	Agente de Registro
AR	Autoridades de Registro
CF-e	Cupom Fiscal Eletrônico
CFTV	Circuito Fechado de Televisão
CG	Comitê Gestor
DPC	Declaração de Práticas de Certificação
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
NBR	Norma Brasileira
OM-BR	Objetos Metrológicos ICP-Brasil
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócios
PIN	Personal Identification Number
PS	Política de Segurança
SAT	Sistema de Autenticação e Transmissão
SSL	Secure Socket Layer
VPN	Virtual Private Network

1 DISPOSIÇÕES GERAIS

1.1 Este documento tem por finalidade regulamentar os procedimentos mínimos a serem adotados pelas Autoridades de Registro - AR da ICP-Brasil. Suplementa, para essas entidades, os regulamentos contidos no documento DOC-ICP-05 [1], tomando como base também a Política de Segurança da ICP-Brasil, DOC-ICP-02 [2].

1.2 Esses regulamentos aplicam-se a todas as AR integrantes da ICP-Brasil.

1.3 Para o presente documento aplicam-se os seguintes conceitos:

a) **Agente de registro** – Pessoa responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a identificação dos requerentes na solicitação de certificados. Essa pessoa também é identificada nos normativos da ICP-Brasil pela sigla AGR.

b) **Autoridade de registro** - Entidade responsável pela interface entre o usuário e a Autoridade Certificadora - AC. É sempre vinculada a uma AC e tem por objetivo o recebimento, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes.

c) **Confirmação da identidade de um indivíduo** - Comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada.

d) **Confirmação da identidade de uma organização** - Comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição.

e) **Desligamento de um Agente de Registro** – Ocorre nas seguintes hipóteses:

i. quando um funcionário ou servidor que tenha recebido a função de Agente de Registro é demitido ou exonerado da organização;

ii. quando um funcionário ou servidor que tenha recebido a função de Agente de Registro deixa de exercê-la em caráter permanente, mesmo que continue trabalhando na organização da AR.

f) **Dossiê do Agente de Registro** – Conjunto de documentos relativos ao Agente de Registro: comprovante de escolaridade, de residência, certificados de treinamento, comprovantes de verificação de antecedentes, e outros citados nos itens 2.2.1 e 2.2.2 deste documento.

g) **Dossiê do titular de certificado** – Conjunto formado pelas verificações dos documentos de identificação utilizados para emissão do certificado e pelos termos de titularidade digitais, e pela solicitação de revogação, quando for o caso. Este dossiê deverá ser no formato de arquivo digital, em que os documentos sejam digitalizados e o termo de titularidade assinado com a chave privada do titular, após a autorização pelo agente de registro por meio de assinatura no referido termo, desde que seja dada ciência e aceitação do seu conteúdo pelo seu requerente e assinado digitalmente após a geração das chaves,

concomitante a requisição do certificado digital, e anterior à instalação do certificado correspondente.

h) **Emissão do certificado** - Conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.

i) **Ponto de Centralização da AC** – Local único, em território nacional, onde a AC armazena, cópia dos dossiês de todos os Agentes de Registro das AR vinculadas. Armazena, também, os dossiês de titulares de certificados da ICP-Brasil.

j) **Suspensão de um Agente de Registro** – Ocorre quando um funcionário ou servidor que tenha recebido a função de Agente de Registro deixa de exercê-la em caráter temporário. A suspensão somente implica a alteração das permissões do Agente de Registro no sistema da AC, não sendo necessário realizar entrevista de desligamento nem assinatura de termos de desligamento.

k) **Identificação da solicitação de certificado** – Compreende a etapa de confirmação da identidade de um individuo ou de uma organização, realizada mediante a presença física do interessado, com base nos documentos de identificação, e a etapa de emissão do certificado, conforme DOC-ICP-05 [1].

l) **Assinatura digital do termo de titularidade** - Documento eletrônico assinado digitalmente após a geração das chaves, concomitante à requisição do certificado digital e anterior à instalação do certificado correspondente, utilizando exclusivamente uma das suítes de assinatura definidas no DOC-ICP-01.01 [7], conforme definido na RFC 8017 (PKCS#1), com o hash, SHA-256 ou superior, da chave pública inserido no documento.

1.4 Os critérios e procedimentos para credenciamento de uma AR estão definidos no documento DOC-ICP-03 [3].

1.5 Somente poderão emitir certificados da ICP-Brasil as Autoridades de Registro que estejam devidamente credenciadas junto à ICP-Brasil conforme despacho publicado no Diário Oficial da União.

1.6 O cumprimento das regras constantes deste documento será verificado por meio de auditorias e fiscalizações, realizadas consoante documentos DOC-ICP-08 [5] e DOC-ICP-09 [6].

1.7 Em caso de alteração de endereço da AR, o fato deve ser previamente reportado à AC responsável, que enviará ao ITI formulário de credenciamento ADE-ICP-03.B [4] com dados atualizados.

2 SEGURANÇA DE PESSOAL

2.1 Disposições Gerais

2.1.1 Os normativos que tratam da segurança de pessoas estão descritos no DOC-ICP-02 [2] e no DOC-ICP-05 [1].

2.1.2 Não são admitidos estagiários nem funcionários terceirizados no exercício das atividades de Agente de Registro. Os Agentes de Registro devem ser funcionários ou servidores da própria organização credenciada como AR junto à ICP-Brasil.

2.1.2.1 Os funcionários das serventias extrajudiciais autorizadas pelo Conselho Nacional de Justiça podem atuar como AGR desde que seja formalizado um contrato com uma AR com, no mínimo, as seguintes cláusulas:

i. qualificação da AR credenciada e do titular da delegação do serviço notarial e de registro;

ii. objeto detalhado das atividades a serem desenvolvidas;

iii. responsabilidade objetiva e solidária do titular da delegação e da AR pelas atividades de identificação da solicitação de certificados;

iv. compromisso de respeitar todas as regras da ICP-Brasil;

v. obrigação de a AR verificar a conformidade dos processos da ICP-Brasil;

vi. prazo de vigência.

2.1.3 A AR deve enviar à AC a relação atualizada dos Agentes de Registro em atividade, seus perfis qualificados e suas necessidades de acesso a informações do gerenciamento de ciclo de vida dos certificados. A AC deve manter essa informação atualizada, organizada e consolidada, inclusive com o histórico das alterações realizadas, à disposição do ITI para os procedimentos de auditoria e fiscalização.

2.2 Documentação do Agente de Registro

2.2.1 Cada Agente de Registro que esteja atuando ou que já tenha atuado na AR deve possuir um dossiê, contendo:

a) contrato de trabalho ou cópia das páginas da carteira de trabalho onde consta o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;

b) comprovante da verificação de antecedentes criminais;

c) comprovante da verificação de situação de crédito;

d) comprovante da verificação de histórico de empregos anteriores;

e) comprovação de escolaridade e de residência;

f) comprovante dos treinamentos realizados;

g) resultado da entrevista inicial, com a assinatura do entrevistador;

h) declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir a Política de Segurança - PS da AC, as políticas e regras aplicáveis da ICP-Brasil. Nessa declaração assume também o dever de manter a confidencialidade e exclusividade de propriedade das informações disponibilizadas pela AC à AR e de manter sigilo, mesmo quando desligado da AR, sobre todas as informações e os processos executados na AR;

i) resultado da avaliação periódica, prevista no DOC-ICP-02 [2];

j) confirmação da AC quanto à inclusão do Agente em seu sistema de certificação.

2.2.2 Caso o Agente de Registro tenha sido desligado de suas atividades na AR, seu dossiê deve conter, também:

a) confirmação da AC quanto à desabilitação do Agente de Registro no sistema de certificação e no Cadastro de Agentes de Registros - CAR mantido no site do ITI;

b) declaração assinada pelo Agente de Registro de que não possui pendências, conforme previsto no item referente ao processo de liberação do DOC-ICP-02 [2];

c) resultado da entrevista de desligamento, com a assinatura do entrevistador;

2.2.3 Os documentos 2.2.1.a até 2.2.1.h, que compõem o dossiê, devem ser examinados por uma das seguintes pessoas, que declarará, sob as penas da lei, a existência de tais documentos e que eles comprovam efetivamente que o Agente de Registro atende a todos os requisitos da ICP-Brasil pertinentes:

a) Auditor interno da AR, cadastrado junto à ICP-Brasil conforme DOC-ICP-08 [5];

b) Auditor ou funcionário designado da Autoridade Certificadora à qual a AR se vincula;

c) Representante Legal da própria AR, caso a AR não possua agente de registro como sócio.

2.2.4 Somente após o recebimento da solicitação de habilitação do Agente de Registro e da declaração prevista no item anterior, a AC pode incluí-lo nas bases de dados e conceder as permissões de acesso no sistema de certificação, sendo necessária para isso prévia autorização documentada do Gerente da AC ou do responsável por ele designado.

2.2.5 Os dossiês de todos os Agentes de Registro da AR devem ficar em um mesmo ponto de centralização da AC, que será informado ao ITI.

2.3 Treinamento

2.3.1 Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, com carga horária mínima de 16 (dezesseis) horas, sobre os seguintes temas:

a) princípios e mecanismos de segurança da AR;

b) sistema de certificação em uso na AC;

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

d) reconhecimento de assinaturas e validade dos documentos apresentados;

e) outros assuntos relativos a atividades sob sua responsabilidade.

2.3.2 No treinamento sobre princípios e mecanismos de segurança devem ser apresentados a Política de Segurança da AC, suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

2.3.3 O treinamento em reconhecimento de assinaturas e validade dos documentos apresentados deve ser ministrado (ou preparado, quando se tratar de treinamentos tipo *e-learning*) por empresa ou profissional especializado em grafotecnia.

2.4 Acompanhamento periódico

2.4.1 A AR deve acompanhar o desempenho das funções de seus Agentes de Registro e avaliá-los anualmente com o propósito de detectar a necessidade de atualização técnica e de segurança. Esse processo deve ser documentado.

2.4.2 A AR deve renovar bianualmente, para todos os seus Agentes de Registro, as verificações de antecedentes criminais e situação creditícia.

2.4.3 Para os casos em que o acompanhamento anual apontar a necessidade de suspensão ou desligamento do Agente de Registro, essa deve ser de imediato solicitada à AC.

2.4.4 A AC deve arquivar os comprovantes relativos aos procedimentos acima no dossiê dos Agentes de Registro em seu poder.

2.5 Suspensão e Desligamento

2.5.1 Quando o Agente de Registro é suspenso ou desligado de suas atividades, a AR imediatamente providencia a revogação de suas permissões de acesso ao sistema de certificação da AC e permissões de acesso físico e lógico aos equipamentos e mecanismos inerentes à atividade de Agente de Registro. Esses processos devem ser documentados e esses documentos devem ser arquivados no dossiê do Agente, os quais deverão ser mantidos em poder da AC.

3 SEGURANÇA FÍSICA

3.1 As atividades da AR relativas à identificação da solicitação de certificados devem ser executadas observando o disposto nos itens que tratam de Identificação e Autenticação no DOC-ICP-05 [1].

3.2 A manutenção preventiva/corretiva das estações de trabalho da AR deve ser realizada apenas por agentes autorizados (pelo fabricante, por assistência técnica autorizada ou por pessoa designada pela AC), dentro do período de manutenção recomendado. Os eventos de manutenção devem ser documentados.

4 SEGURANÇA LÓGICA

4.1 Estações de trabalho

4.1.1 As estações de trabalho da AR, incluindo equipamentos portáteis, devem estar protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos.

4.1.1.1 A(s) partição(ões) dos discos rígidos das estações de trabalho da AR que contém componentes da aplicação da AC/AR ou que armazenem dados de solicitantes de certificados digitais devem ser criptografadas; ou políticas de segurança devem ser aplicadas as estações de trabalho da AR de forma a não permitir a gravação de arquivos locais nestes equipamentos.

4.1.1.2 As estações de trabalho da AR devem implementar aplicação que faça controle de integridade das configurações da aplicação de AR, bem como dos arquivos de configuração ou informações críticas mantidas na estação de trabalho.

4.1.1.3 As estações de trabalho da AR deverão conter apenas aplicações e serviços que sejam suficientes e necessários para as atividades corporativas.

4.1.2 As estações de trabalho da AR, incluindo equipamentos portáteis, devem receber, pelo menos, as seguintes configurações de segurança:

a) controle de acesso lógico ao sistema operacional;

b) diretivas de senha e de bloqueio de conta;

c) *logs* de auditoria do sistema operacional ativados, registrando:

i. iniciação e desligamento do sistema;

ii. tentativas de criar, remover, definir senhas ou mudar privilégios de usuários;

iii. mudanças na configuração da estação;

iv. tentativas de acesso *(login)* e de saída do sistema *(logoff);*

v. tentativas não-autorizadas de acesso aos arquivos de sistema;

vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.

d) antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;

e) *firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes que possuam esse dispositivo;

f) proteção de tela acionada no máximo após dois minutos de inatividade;

g) sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);

h) utilização apenas de *softwares* licenciados e necessários para a realização das atividades do AGR;

i) impedimento de *login* remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;

j) utilização de data e hora de Fonte Confiável do Tempo (FCT);

k) equipamentos de coleta biométrica, em atendimento aos padrões da ICP-Brasil;

l) equipamentos que exijam a identificação biométrica do agente de registro durante a identificação biométrica do requerente do certificado;

m) Módulo de segurança, software assinado pela AC, que garanta a integridade e a segurança da estação de trabalho.

4.1.3 Os *logs* de auditoria do sistema operacional devem registrar os acessos aos equipamentos e devem ficar armazenados localmente para avaliação pela auditoria operacional ou equipe de segurança.

4.1.4 A análise desses *logs* deve ser realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

4.1.5 O Agente de Registro não deve possuir perfil de administrador ou senha de *root* dos equipamentos ou com privilégios especiais do sistema, ficando essa tarefa delegada a outros da própria organização, para permitir segregação de funções. O Agente de Registro somente deve receber acesso aos serviços e aplicações que tenham sido especificamente autorizados a usar.

4.2 Aplicativo da AR

4.2.1 O aplicativo que faz interface entre a AR e o sistema de certificação da AC deve possuir pelo menos as seguintes características de segurança:

a) acesso permitido somente mediante autenticação por meio do certificado do tipo A3 de Agente de Registro, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC;

b) acesso permitido somente a partir de equipamentos autenticados no sistema (ex. usando cadastramento prévio de endereço IP, certificado digital de equipamento ou outra solução que permita ao sistema identificar de forma unívoca o equipamento);

c) *timeout* de sessão de acordo com a análise de risco da AC;

d) registro em *log* de auditoria dos eventos citados no item “Tipos de eventos registrados” do DOC-ICP-05 [1];

e) histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;

f) mecanismo para revogação automática dos certificados digitais.

4.2.2 Para atendimento do previsto no DOC-ICP-05 [1] para Geração e Instalação do Par de Chaves, esse aplicativo deve:

a) ter sido desenvolvido com documentação formal;

b) ter mecanismos para controle de versões;

c) ter documentação dos testes realizados em cada versão;

d) ter documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si;

e) ter aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção;

4.2.3 Os *logs* gerados por esse aplicativo devem ser armazenados na AC pelo prazo de 7 anos.

5 SEGURANÇA DE REDE

5.1 A AR deve encaminhar as solicitações de emissão ou de revogação de certificados à AC utilizando VPN (*Virtual Private Network* - rede privativa virtual), SSL (S*ecure Socket Layer* - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.

6 SEGURANÇA DA INFORMAÇÃO

6.1 Diretrizes Gerais

6.1.2 A AC deve possuir um dossiê, contendo o seguinte:

a) Relação dos Agentes de Registro que estejam atuando ou já tenham atuado na AR com respectivos nº de CPF;

b) Topologia de Rede de Comunicação entre a AR e a AC;

c) Manual Operacional do Agente de Registro;

d) Inventário de Ativos;

e) Plano de Continuidade de Negócios;

f) Análise de Risco.

6.1.3 A Análise de Risco e o Plano de Continuidade de Negócios devem ser elaborados de acordo com o disposto no DOC-ICP-02 [2].

6.1.4 A AR deve possuir, também, cópia do PCN.

6.1.5 O Inventário de Ativos deve estar sempre atualizado, mantendo histórico das alterações e deve ser assinado pelo responsável pela AR.

6.1.6 O Inventário de Ativos deve relacionar, pelo menos:

a) equipamentos da AR, com respectivas especificações, atualizado mensalmente;

b) *softwares* instalados nos equipamentos, atualizado mensalmente;

6.1.6.1 Somente poderão constar do Inventário de Ativos os equipamentos de propriedade ou de posse da AR.

6.1.6.2 A comprovação da posse ou propriedade dos equipamentos a que se refere o item anterior deverá ser feita sempre que assim requisitado pela AC Raiz, mediante a apresentação pela AR da respectiva nota fiscal, comodato, leasing, doação, contrato de locação de equipamentos ou documentação comprobatória equivalente.

6.2 Armazenamento, manuseio, guarda e destruição de documentos

6.2.1 Os documentos que compõem os dossiês dos titulares de certificados e dos agentes de registro AR devem ser enviados à AC vinculada, inclusive os antigos, e guardados, preferencialmente, em ambiente computacional protegido, com acesso permitido somente aos agentes de registro vinculados ou responsáveis designados formalmente para trabalhar com os documentos.

6.2.2 A AC pode substituir a guarda física dos documentos que compõem o dossiê do Agente de Registro e o dossiê do Titular do Certificado por digitalização dos mesmos, observado que:

a) documentos cuja cópia deva constar no dossiê (ex.: documentos de identificação apresentados pelo titular, carteira de trabalho do Agente de Registro etc.) devem ser digitalizados e assinados digitalmente com o certificado ICP-Brasil;

b) documentos cujo original deva constar do dossiê (ex.: termos de titularidade, declarações do Agente de Registro etc.) podem ser digitalizados para inclusão no dossiê respectivo, devendo permanecer arquivados no ponto de centralização da AC pelo prazo estipulado nas resoluções da ICP-Brasil;

c) todos os arquivos que compõem um dossiê devem ser organizados de forma a permitir sua recuperação conjunta, para fins de fiscalização e auditoria;

d) o diretório ou sistema onde são armazenados esses arquivos deve ter proteção contra leitura e gravação, dando permissão de acesso somente aos Agentes de Registro vinculados ou responsáveis designados formalmente para trabalhar com os documentos;

e) devem ser especificados procedimentos de cópia e recuperação em caso de sinistro.

6.2.2.1 Os originais, referenciados na alínea “b”, do item 6.2.2, poderão ser destruídos desde que o processo de digitalização tenha sido realizado com o emprego de certificado digital emitido no âmbito da ICP - Brasil. Nessa hipótese o documento digitalizado deverá ser assinado com o certificado da entidade da ICP-Brasil que fez a conferência da integridade do documento digitalizado.

6.2.2.2 Caso a digitalização seja realizada pela AR, esta deverá emitir um recibo contendo a identificação de todos os dossiês digitalizados encaminhados para a AC. Após a conferência dos dossiês digitalizados a AC deverá assinar o recibo.

6.2.3 O armazenamento definitivo dos dossiês de titulares de certificado, digitalizados ou eletrônicos, deve ser feito:

a) no ponto de centralização da AC à qual a AR está vinculada; ou

b) na AC emissora para os casos de certificados A CF-e-SAT ou OM-BR.

6.2.4 A remessa ou transmissão do dossiê para o local de armazenamento definitivo deve ser feita por meio seguro (ex.: remessa com aviso de recebimento para documentos em papel e transmissão via VPN para documentos digitalizados ou eletrônicos), no prazo máximo de 7 (sete) dias corridos, a partir da geração do dossiê.

6.2.5 A AC deve utilizar sistema que permita determinar, facilmente e a qualquer momento, o local onde se encontra cada dossiê de titular de certificados que se encontra sob sua guarda.

6.2.6 O Ponto de Centralização da AC deve ser informado ao ITI, bem como qualquer alteração que venha a ser feita posteriormente.

6.2.7 Todos os documentos em papel que contenham informações classificadas como sensíveis devem ser destruídos, de forma a tornar irrecuperável a informação neles contida, antes de ir para o lixo. Incluem-se nessa categoria as cópias não utilizadas de documentos dos titulares de certificados, termos de titularidade descartados, diagramas de rede, etc.

6.2.8 Quando da exclusão de arquivos contendo cópias de documentos dos dossiês de titulares de certificados deve ser realizado o completo apagamento, inclusive com limpeza da lixeira, de forma a impedir sua recuperação e uso indevidos.

6.2.9 O dossiê do titular do certificado A CF-e-SAT ou OM-BR deve conter toda a documentação eletrônica utilizada no processo de validação da solicitação e o termo de titularidade específico assinado digitalmente com um certificado digital ICP-Brasil de pessoa jurídica, conforme regulamentado na PC do A CF-e-SAT e do OM-BR.

7 CICLO DE VIDA DO CERTIFICADO

7.1 Os processos que dizem respeito ao ciclo de vida do certificado - solicitação, identificação da solicitação, emissão e revogação - estão descritos no documento DOC-ICP-05.

8 DAS VEDAÇÕES

8.1 É vedada, por parte das AC e AR credenciadas junto à AC Raiz, a divulgação, anúncio ou qualquer outra forma de publicidade de atividades, serviços ou produtos relacionados com o comércio de certificado digital da ICP-Brasil que não estejam normatizados e autorizados pela ICP-Brasil.

8.2 É vedada qualquer outra forma de emissão de certificado, fora das hipóteses não expressamente previstas na legislação e nas normas que regem a ICP-Brasil.

8.3 É vedado delegar ou transferir a terceiros, não credenciados, atividades privativas das entidades credenciadas ou autorizadas pelo ITI, a qualquer título.

8.4 No caso de descumprimento das normas de emissão de certificado, poderá o ITI determinar a revogação imediata do certificado digital emitido em desconformidade com as normas que regem a ICP-Brasil, que não tenham atendido os requisitos estabelecidos na regulamentação, ressalvado o direito de terceiros de boa-fé.

9 DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[2]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[5]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

9.2 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]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[4]	FORMULÁRIO DE CREDENCIAMENTO DE AR	ADE-ICP-03.B

Anexo IV

Infraestrutura de Chaves Públicas Brasileira

REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL

DOC-ICP-04

Versão 7.0

30 de maio de 2019

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
Resolução 151 de 30.05.2019 (versão 7.0)		Aprova a versão 7.0 do DOC-ICP-04.
Resolução 150 de 07.11.2018 (versão 6.7)	7.1.4.1,	Inclui no certificado digital o CNPJ da Autoridade de Registro onde ocorreu a identificação presencial.
Resolução 141 de 03.07.2018 (versão 6.6)	7.1.2.3-a	Incluir os servidores públicos dos estados e do Distrito Federal nos procedimentos específicos de emissão de certificados digitais.
Resolução 139 de 03.07.2018 (versão 6.6)	1.1.3, 1.1.7A, 1.1.8, 1.2.2, 1.3.5.8, 6.1.1.1.2, 6.1.1.7, 6.1.8, 6.2.4.1, 6.3.2.3, 7.1.2.3, Tabela do Anexo I	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
Resolução 138 de 02.04.2018 (versão 6.5)	7.1.2.3 e 7.1.2.4	Alteração da extensão "subject alternative name" para certificados de equipamento A CF-e-SAT.
Resolução 132 de 10.11.2017 (versão 6.4)	1.3.3A, 6.2.4.2	Institui o Prestador de Serviço de Confiança.
Resolução 128 de 13.09.2017 (versão 6.3)	7.1.2.3.c	Obriga certificados do tipo SSL/TLS a incluírem o Campo dNSName da extensão Subject Alternative Name.
Resolução 124 de 13.09.2017 (versão 6.3)	7.1.2.8	Retira a proibição de certificados A CF-e-SAT de implementar a extensão Extended Key Usage.
Resolução 119, 121 e 123 de 06.07.2017 (versão 6.2)	7.1.2.2.e, 7.1.2.3.a.4 e 6.1.1 Tabela 4 e Anexo I	Obrigação de resposta OCSP para certificados de autenticação de servidor (SSL/TLS). Inclui a previsão para certificados para servidor público federal e militar. Atualiza tabela de mídias armazenadoras de chaves criptográficas e tabela Comparativa de Requisitos Mínimos por Tipo de Certificado.

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
Resolução 118, de 09.12.2015 (versão 6.1)	7.1.2.2 7.2.2.2.c	Previsão de dois pontos para obtenção da LCR. Retirada do campo AIA da LCR.
Resolução 115, de 11.11.2015 (versão 6.0)	1.1.3, 1.1.7, 1.1.8, tabela 3, 1.3.5.7, 6.1.1.1.1, tabela 4, tabela 5, 6.2.4.1, tabela 6, 7.1.2.3, 7.1.2.8 e anexo I.	Cria nova política de certificado A CF-e-SAT.
Resolução 103, de 29.04.2014 (versão 5.3)	7.1.2.2-e; 7.1.2.7; 7.1.2.3-a.a1.i; 7.1.2.3-b.i; 7.1.2.4-f.	Esclarece uso da extensão *ExtendedKeyUsage* nos certificados de usuário final e ajusta o campo de RG na extensão *"Subject Alternative Name"*.
Resolução 99, de 09.10.2013 (versão 5.2)	Tabela 6 item 6.3.2.3; Tabela do Anexo I.	Amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolução 95, de 27.09.2012 (versão 5.1)	Tabela 4 do item 6.1.1.7; Tabela do Anexo I.	Adequação das exigências vinculadas aos equipamentos, para certificados do tipo T3 e T4.
Resolução 91, de 05.07.2012 (versão 5.0)	Tabela 6 do item 6.3.2.3; Tabela do Anexo I; alíneas "iii" do subitem "b" e "ii" do subitem "c", do item 7.1.2.3	Alteração do Período máximo de Validade dos Certificados A3, S3, T3 para 5 anos e do Tamanho (bits) da Chave Criptográfica. Inclusão das 14 pos. no CNPJ para o OID 2.16.76.1.3.3.
Resolução 87, de 17.04.2010 (versão 4.0)	7.1.2.3-a; Tabela 4 do item 6.1.1.7; Tabela 6 do item 6.3.2.3; Tabela do Anexo I.	Ajuste em redação para campos *otherName* e alteração de validade de certificados de tipo A4, S4 e T4 para 6 anos, com restrição de armazenamento em hardware criptográfico.
Resolução 84, de 18.11.2010 (versão 3.2)	7.1.2.3-a	Inclusão de campo *otherName*, obrigatório para certificado vinculado ao RIC
Resolução 77, de 31.03.2010 (Versão 3.1)	7.1.2.2-e, 7.1.2.2-f, 7.2.2.2-c	Inclusão do campo de extensão de Authority Information Access
Resolução 53, de 19.11.2008 (Versão 3.0)	1.1.3, 1.1.6, 1.2.2, 1.3.5.6, 6.1.1.7, 6.1.8, 6.2.4.1, 6.3.2.3, 7.1.2.2, 7.1.4.2, Anexo I	Inclusão de referências a Carimbo de Tempo
	7.1.2.4	Inclusão do formato PRINTABLE STRING como alternativa ao formato OCTET STRING para armazenamento das informações definidas nos campos otherName

Resolução que aprovou alteração	Item Alterado	Descrição da Alteração
Resolução 41, de 18.04.2006 (Versão 2.0)	Diversos	Consolidação de documentos anteriores
Resolução 07, de 12.12.2001 (Versão 1.0)	Diversos	Criação do DOC-ICP-04

TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology

SIGLA	DESCRIÇÃO
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

1 INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1 Visão Geral

1.1.1 Este documento estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras – AC integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na elaboração de suas Políticas de Certificado (PC).

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

1.1.3 São 12 (doze) os tipos, inicialmente previstos, de certificados digitais para usuários finais da ICP-Brasil, sendo 8 (oito) relacionados com assinatura digital e 4 (quatro) com sigilo, conforme o descrito a seguir:

a) Tipos de Certificados de Assinatura Digital:

A1

A2

A3

A4

T3

T4

A CF-e-SAT

OM-BR

b) Tipos de Certificados de Sigilo:

i. S1

ii. S2

iii. S3

iv. S4

1.1.4 Os tipos de certificados indicados acima, de A1 a A4 e de S1 a S4, definem escalas de requisitos de segurança, nas quais os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos.

1.1.5 Certificados dos tipos de A1 a A4 e de S1 a S4, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

1.1.6 Certificados do tipo T3 e T4 somente podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil. Os certificados do tipo T3 e T4 estão associados aos mesmos requisitos de segurança, exceto pelo tamanho das chaves criptográficas utilizadas.

1.1.7 Certificados do tipo A CF-e-SAT só podem ser emitidos para equipamentos integrantes do Sistema de Autenticação e Transmissão do Cupom Fiscal Eletrônico - SAT-CF-e, seguindo a regulamentação do CONFAZ.

1.1.8 Certificados do tipo Objeto Metrológico - OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo Inmetro.

1.1.9 Outros tipos de certificado, além dos doze anteriormente relacionados, podem ser propostos para a apreciação do Comitê Gestor da ICP-Brasil – CG da ICP-Brasil. As propostas serão analisadas quanto à conformidade com as normas específicas da ICP-Brasil e, quando aprovadas, serão acrescidas aos tipos de certificados aceitos pela ICP-Brasil.

1.1.10 Para certificados com propósito de uso EV SSL e EV CS devem ser observados os dispostos nos documentos EV SSL/CS Guidelines.

1.2 Nome do documento e identificação

1.2.1 Neste item deve ser identificada a PC e indicado, no mínimo, o tipo de certificado a que está associada. Exemplo: "Política de Certificado de Assinatura Digital, tipo A1, do(a) <*nome da instituição*>". O OID (*Object Identifier*) da PC deve também ser incluído neste item.

1.2.2 No âmbito da ICP-Brasil, os OIDs das PCs serão atribuídos na conclusão do processo de credenciamento da AC, conforme a Tabela 3 a seguir:

Tabela 3 - OID de PC na ICP-Brasil

Tipo de Certificado	*OID*
A1	2.16.76.1.2.1.*n*
A2	2.16.76.1.2.2.*n*
A3	2.16.76.1.2.3.*n*
A4	2.16.76.1.2.4.*n*
S1	2.16.76.1.2.101.*n*
S2	2.16.76.1.2.102.*n*
S3	2.16.76.1.2.103.*n*
S4	2.16.76.1.2.104.*n*
T3	2.16.76.1.2.303.*n*
T4	2.16.76.1.2.304.*n*

A CF-e-SAT	2.16.76.1.2.500.n
OM-BR	2.16.76.1.2.550.n

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

1.3.1.1 Neste item deve ser identificada a AC integrante da ICP-Brasil que implementa a PC.

1.3.1.2 Deve também ser identificado o documento Declaração de Práticas de Certificação (DPC) dessa AC, onde estarão descritas suas práticas e procedimentos de certificação.

1.3.2 Autoridades de Registro

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

a) relação de todas as ARs credenciadas;

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

1.3.3 Titulares do Certificado

Neste item devem ser caracterizadas as entidades (pessoas físicas ou jurídicas, equipamentos ou aplicações) que poderão ser titulares dos certificados emitidos segundo a PC.

1.3.4 Partes Confiáveis

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

1.3.5 Outros Participantes

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

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

1.4.1.1 Neste item devem ser relacionadas as aplicações para as quais os certificados definidos pela PC são adequados..

1.4.1.2 As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3 Na definição das aplicações para o certificado definido pela PC, a AC responsável deve levar em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado.

1.4.1.4 Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.

1.4.1.6 Certificados de tipos T3 e T4 serão utilizados em aplicações mantidas por autoridades de carimbo do tempo credenciadas na ICP-Brasil, para assinatura de carimbos do tempo.

1.4.1.7 Certificados de tipo A CF-e-SAT serão utilizados exclusivamente em equipamentos para assinatura de Cupom Fiscal Eletrônico – CF-e por meio do Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico – SAT.

1.4.1.8 Certificados do tipo OM-BR serão utilizados exclusivamente em equipamentos metrológicos regulamentados pelo Inmetro.

1.4.2 Uso proibitivo do certificado

Neste item devem ser relacionadas, quando cabível, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.5 Política de Administração

Neste item devem ser incluídos nome, endereço e outras informações da AC responsável pela PC. Devem ser também informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC.

1.5.2 Contatos

Endereço:
Telefone:
Fax:
Página web:
E-mail:
Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome:
Telefone:
E-mail:
Outros:

1.5.4 Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.
Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da 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	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoas Físicas
CS	*Code Signing*
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	*Extended Validation*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados

SIGLA	DESCRIÇÃO
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
NIS	Número de Identificação Social
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OM-BR	Objetos Metrológicos ICP-Brasil
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
SSL	*Secure Socket Layer*
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

2.1 Repositórios

2.2 Publicação de informações dos certificados

2.3 Tempo ou Frequência de Publicação

2.4 Controle de Acesso aos Repositórios

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

3.1 Nomeação

3.1.1 Tipos de nomes

3.1.2 Necessidade dos nomes serem significativos

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.5 Unicidade de nomes

3.1.6 Procedimento para resolver disputa de nomes

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

3.2 Validação inicial de identidade

3.2.1 Método para comprovar a posse de chave privada

3.2.2 Autenticação da identificação da organização

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

4.4.2 Publicação do certificado pela AC

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

4.5 Usabilidade do par de chaves e do certificado

4.5.1 Usabilidade da Chave privada e do certificado do titular

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

4.6 Renovação de Certificados

4.6.1 Circunstâncias para renovação de certificados

4.6.2 Quem pode solicitar a renovação

4.6.3 Processamento de requisição para renovação de certificados

4.6.4 Notificação para nova emissão de certificado para o titular

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6 Publicação de uma renovação de um certificado pela AC

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

4.7 Nova chave de certificado

4.7.1 Circunstâncias para nova chave de certificado

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

4.7.3 Processamento de requisição de novas chaves de certificado

4.7.4 Notificação de emissão de novo certificado para o titular

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

4.7.6 Publicação de uma nova chave certificada pela AC

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

4.8 Modificação de certificado

4.8.1 Circunstâncias para modificação de certificado

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3 Processamento de requisição de modificação de certificado

4.8.4 Notificação de emissão de novo certificado para o titular

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

4.8.6 Publicação de uma modificação de certificado pela AC

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

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

4.9.2 Quem pode solicitar revogação

4.9.3 Procedimento para solicitação de revogação

4.9.4 Prazo para solicitação de revogação

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

4.9.7 Frequência de emissão de LCR

4.9.8 Latência máxima para a LCR

4.9.9 Disponibilidade para revogação/verificação de status on-line

4.9.10 Requisitos para verificação de revogação on-line

4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.13 Circunstâncias para suspensão

4.9.14 Quem pode solicitar suspensão

4.9.15 Procedimento para solicitação de suspensão

4.9.16 Limites no período de suspensão

4.10 Serviços de status de certificado

4.10.1 Características operacionais

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável ou detalhados aspectos específicos para a PC, se houver.

5.3 Controles de Pessoal

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2 Procedimentos de verificação de antecedentes

5.3.3 Requisitos de treinamento

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.5 Frequência e sequência de rodízio de cargos

5.3.6 Sanções para ações não autorizadas

5.3.7 Requisitos para contratação de pessoal

5.3.8 Documentação fornecida ao pessoal

5.4 Procedimentos de Log de Auditoria

5.4.1 Tipos de eventos registrados

5.4.2 Frequência de auditoria de registros

5.4.3 Período de retenção para registros de auditoria

5.4.4 Proteção de registros de auditoria

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

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

5.4.7 Notificação de agentes causadores de eventos

5.4.8 Avaliações de vulnerabilidade

5.5 Arquivamento de Registros

5.5.1 Tipos de registros arquivados

5.5.2 Período de retenção para arquivo

5.5.3 Proteção de arquivo

5.5.4 Procedimentos de cópia de arquivo

5.5.5 Requisitos para datação de registros

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

5.5.7 Procedimentos para obter e verificar informação de arquivo

5.6 Troca de chave

5.7 Comprometimento e Recuperação de Desastre

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

5.8 Extinção da AC

6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC deve definir as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC. Devem também ser definidos outros controles técnicos de segurança utilizados pela AC e pelas ARs vinculadas na execução de suas funções operacionais.

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

6.1.1.1 Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1 Para certificados do tipo A CF-e-SAT, o titular do certificado será o contribuinte, que fará a solicitação do certificado A CF-e-SAT com uso de certificado digital ICP-Brasil de pessoa jurídica válido e correspondente ao mesmo CNPJ para o qual está autorizado pela unidade fiscal federada, associado ao número de série do equipamento SAT.

6.1.1.1.2 Para certificados do tipo OM-BR, o titular do certificado será o fabricante, que fará a solicitação do certificado OM-BR com uso de certificado digital ICP-Brasil de pessoa jurídica válido, do fabricante autorizado pelo Inmetro.

6.1.1.2 Neste item, a PC deve descrever todos os requisitos e procedimentos referentes ao processo de geração de chaves aplicável ao certificado que define.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.1.4 Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1], no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 4 a seguir.

6.1.1.5 A chave privada deverá trafegar cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

6.1.1.6 A mídia de armazenamento da chave privada deverá assegurar, por meios técnicos e procedimentais adequados, no mínimo, que:

a) a chave privada é única e seu sigilo é suficientemente assegurado;

b) a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 Essa mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do DOC-ICP-17 [4], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

Tabela 4 – Mídias Armazenadoras de Chaves Criptográficas

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (Requisitos Mínimos)
A1 e S1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima
A2 e S2	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica
A3 e S3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A4 e S4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
T3 e T4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A CF-e-SAT	Hardware criptográfico.
OM-BR	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

Nota: para certificados do tipo A CF-e-SAT, T3 e T4, a exigência de homologação ou certificação das mídias para geração e armazenamento de chaves criptográficas fica suspensa até ulterior deliberação do Comitê Gestor da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade

Item não aplicável.

6.1.3 Entrega da chave pública para emissor de certificado

A PC deve detalhar os procedimentos utilizados para a entrega da chave pública de titular de certificado à AC responsável. Nos casos em que houver solicitação de certificado pelo seu titular ou por AR vinculada, deverá ser adotado formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.4 Entrega de chave pública da AC às terceiras partes

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

a) no momento da disponibilização de um certificado para seu titular; usando formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1];

b) diretório;

c) página *web* da AC; e

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

6.1.5 Tamanhos de chave

6.1.5.1 Este item deve definir o tamanho das chaves criptográficas associadas aos certificados emitidos segundo a PC.

6.1.5.2 Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

A PC deve prever que os parâmetros de geração e verificação de chaves assimétricas das entidades titulares de certificados adotarão o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

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

Neste item, a PC deve especificar os propósitos para os quais poderão ser utilizadas as chaves criptográficas dos titulares de certificados, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes (item 1.4).

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

Nos itens seguintes, a PC deve definir os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos segundo a PC.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 Neste item, quando cabíveis, devem ser especificados os padrões requeridos para os módulos de geração de chaves criptográficas, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.1.2 Este item da PC deve descrever os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado. Poderão ser indicados padrões de referência, observados os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.2.2 Controle "n de m" para chave privada

Item não aplicável.

6.2.3 Custódia (escrow) de chave privada

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

6.2.4 Cópia de segurança de chave privada

6.2.4.1 Com exceção das chaves privadas vinculadas a certificados do tipo A CF-e-SAT, OM-BR, T3 e T4, que não podem possuir cópia de segurança, qualquer titular de certificado dos demais tipos poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC responsável pela PC não poderá manter cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.3 Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [1] e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Além das observações acima, a PC deve descrever todos os requisitos e procedimentos aplicáveis ao processo de geração de uma cópia de segurança.

6.2.5 Arquivamento de chave privada

6.2.5.1 Neste item de uma PC que defina certificados de sigilo, devem ser descritos, quando cabíveis, os requisitos para arquivamento de chaves privadas. Não devem ser arquivadas chaves privadas de assinatura digital.

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

6.2.6 Inserção de chave privada em módulo criptográfico

Neste item, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada de titular em módulo criptográfico.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 Método de ativação de chave privada

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

6.2.9 Método de desativação de chave privada

Neste item da PC devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada de entidade titular. Devem ser definidos os agentes autorizados, o método de confirmação da identidade desses agentes e as ações necessárias.

6.2.10 Método de destruição de chave privada

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A PC deve prever que as chaves públicas de titulares dos certificados de assinatura digital e as LCR serão armazenadas pela AC emissora, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

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

6.3.2.1 Caso a PC se refira a certificados de assinatura digital, ela deve prever que as chaves privadas dos respectivos titulares deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Caso a PC se refira a certificados de sigilo, ela deve definir os períodos de uso das chaves correspondentes.

6.3.2.3 A Tabela 6, a seguir, define os períodos máximos de validade admitidos para cada tipo de certificado previsto pela ICP-Brasil:

Tabela 6 – Períodos de Validade dos Certificados

Tipo de Certificado	*Período Máximo de Validade do Certificado (em anos)*
A1 e S1	1
A2 e S2	2
A3, S3, T3	5
A4, S4, T4	11 (para cadeias hierárquicas completas em Curvas Elípticas)
	6 (para as demais hierarquias)
A CF-e-SAT	5
OM-BR	10

6.3.2.4 O período máximo de validade dos Certificados de Assinatura de Código será de até 39 (trinta e nove) meses, conforme princípios e critérios *Webtrust*.

6.3.2.5 O período máximo de validade dos Certificados SSL/TLS será de até 825 (oitocentos e vinte cinco) dias, conforme princípios e critérios *Webtrust*.

6.4 Dados de Ativação

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

6.4.1 Geração e instalação dos dados de ativação

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

6.4.2 Proteção dos dados de ativação

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

6.4.3 Outros aspectos dos dados de ativação

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

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

A PC deve descrever os requisitos de segurança computacional do equipamento onde serão gerados os pares de chaves criptográficas dos titulares de certificados, observados os requisitos gerais previstos na DPC.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6 Controles Técnicos do Ciclo de Vida

Caso a AC responsável exija um software específico para a utilização dos certificados emitidos segundo a PC, nos itens seguintes devem ser descritos os controles implementados no desenvolvimento e no gerenciamento de segurança referentes a esse software.

6.6.1 Controles de desenvolvimento de sistema

Neste item da PC devem ser abordados aspectos tais como: segurança do ambiente e do pessoal de desenvolvimento, práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros.

6.6.2 Controles de gerenciamento de segurança

Neste item devem ser descritos os procedimentos e as ferramentas empregados para garantir que o software e seu ambiente operacional implementem os níveis configurados de segurança.

6.6.3 Controles de segurança de ciclo de vida

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

6.6.4 Controles na Geração de LCR

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

6.7 Controles de Segurança de Rede

Caso o ambiente de utilização do certificado definido pela PC exija controles específicos de segurança de rede, esses controles devem ser descritos neste item da PC, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

6.8 Carimbo de Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[5].

7 PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes devem especificar os formatos dos certificados e das LCR/OCSP gerados segundo a PC. Devem ser incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os requisitos mínimos estabelecidos nos itens seguintes deverão ser obrigatoriamente atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

7.1 Perfil do certificado

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

7.1.1 Número de versão

Todos os certificados emitidos pela AC responsável, segundo a PC, deverão implementar a versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2 Extensões de certificado

7.1.2.1 Neste item, a PC deve descrever todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões:

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

b) ***"Key Usage"*, crítica**: configurados conforme disposto no item 7.1.2.7 deste documento;

c) ***"Certificate Policies"*, não crítica**: deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado. Certificados de assinatura de código (Code Signing) e de autenticação de servidor (SSL/TLS) devem conter ainda o OID da política de certificado de identificação dos requisitos do *CA/B Forum Guidelines* (2.23.140.1.1, se EV SSL; 2.23.140.1.2.2, se OV SSL; 2.23.140.1.3, se EV Code Signing; e 2.23.140.1.4.1, se Baseline Requirement Code Signing);

d) ***"CRL Distribution Points"*, não crítica**: deve conter 02 (dois) endereços na Web onde se obtém a LCR correspondente;

e) **"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. A segunda entrada deve conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para certificados de autenticação de servidor (SSL/TLS). Todos os outros tipos de certificado podem conter essa segunda entrada. Essas extensões somente são aplicáveis para certificados de usuário final.

7.1.2.3 A ICP-Brasil também define como obrigatória a extensão ***"Subject Alternative Name"*, não crítica**, e com os seguintes formatos:

a) Para certificado de pessoa física:

a.1) 3 (três) campos otherName, obrigatórios, contendo:

OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular; nas 10 (dez)

posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.
OID = 2.16.76.1.3.6 e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.
OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) campos otherName, não obrigatórios, contendo:

OID = 2.16.76.1.4.n e conteúdo = de tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente. A AC Raiz, por meio do documento ATRIBUIÇÃO DE OID NA ICP-BRASIL [2] regulamentará a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.

a.3) 1 (um) campo otherName, obrigatório, para certificados vinculados ao Documento RIC, contendo:

OID = 2.16.76.1.3.9 e conteúdo = nas primeiras 11 (onze) posições, o número de Registro de Identidade Civil.

a.4) 1 (um) campo otherName, obrigatório para certificados digitais emitidos para servidor público e militar, contendo:

OID = 2.16.76.1.3.11 e conteúdo = nas primeiras 10 (dez) posições, o cadastro único do servidor público da ativa e militares da União constante no Sistema de Gestão de Pessoal (SIGEPE) mantido pelo Ministério do Planejamento ou nos sistemas correlatos, no âmbito da esfera estadual e do Distrito Federal, e nos Sistemas de Gestão de Pessoal das Forças Armadas.

b) Para certificado de pessoa jurídica, 4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF;

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado;

OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa jurídica titular do certificado

c) Para certificado de equipamento ou aplicação:

c.1) 4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, se o certificado for de pessoa jurídica;
OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), se o certificado for de pessoa jurídica;

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o número de Identificação Social – NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

c.2) Para certificados do tipo SSL/TLS, Campo dNSName, obrigatório, contendo um ou mais domínios pertencentes ou controlados pelo titular, seguindo as regras definidas na RFC 5280 e RFC 2818, em conformidade com os princípios e critérios *WebTrust*.

d) Para certificado de equipamento A CF-e-SAT, 3 (três) campos otherName, obrigatórios, contendo, nesta ordem:

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, idêntico ao constante no certificado digital de pessoa jurídica requisitante deste ou quando o requisitante for uma Secretaria Estadual da Fazenda, o CNPJ do contribuinte a quem foi atribuído o certificado;

OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), idêntico ao constante no certificado digital de pessoa jurídica requisitante deste ou quando o requisitante for uma Secretaria Estadual da Fazenda, o CNPJ do contribuinte a quem foi atribuído o certificado;

OID = 2.16.76.1.3.10 e conteúdo = nas primeiras 10 (dez) posições, número de série do equipamento emissor de CF-e-SAT; nas 14 (quatorze) posições subsequentes, o número da inscrição estadual da pessoa jurídica emissora do CF-e-SAT; nas 14 (quatorze) posições subsequentes, o número da inscrição municipal da pessoa jurídica emissora do CF-e-SAT.

NOTA: Uma Secretaria Estadual de Fazenda tem a competência institucional de promover a gestão tributária e financeira estadual, bem como supervisionar, coordenar e executar a política tributária e fiscal do Estado.

e) Para certificado de equipamento OM-BR, 3 (três) campos otherName, obrigatórios, contendo, nesta ordem:

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, idêntico ao constante no certificado digital de pessoa jurídica requisitante deste;

OID = 2.16.76.1.3.3 e conteúdo = nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ), idêntico ao constante no certificado digital de pessoa jurídica requisitante deste;

OID = 2.16.76.1.3.12 e conteúdo = nas primeiras 8 (oito) posições, a data de fabricação do equipamento, no formato ddmmaaaa; nas posições subsequentes, os dados de identificação do equipamento." (NR)

7.1.2.4 Os campos otherName definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão

emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas informações de tamanho variável referentes a números, tais como RG, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

h) Quando o número da inscrição estadual e o número da inscrição municipal da pessoa jurídica emissora do CF-e-SAT não estiverem disponíveis não precisam ser preenchidos.

7.1.2.5 Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6 Os outros campos que compõem a extensão *"Subject Alternative Name"* poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7 As extensões "*Key Usage"* e *"Extended Key Usage"* para os referidos tipos de certificado são obrigatórias e devem obedecer os propósitos de uso e a criticalidade conforme descrição abaixo :

a) para certificados de Assinatura de Código (*codeSigning*):
***"Key Usage"*, crítica**: somente o bit *digitalSignature* deve estar ativado;
***"Extended Key Usage", não crítica**:* somente o *codeSigning OID* = 1.3.6.1.5.5.7.3.3 deve estar presente;

b) para certificados de Autenticação de Servidor (*SSL/TLS*):
***"Key Usage"*, crítica**: somente os bits *digitalSignature, keyEncipherment* ou *keyAgreement* podem estar ativado;
***"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;

c) para certificados de Assinatura de Carimbo do Tempo:
***"Key Usage"*, crítica**: somente os bits *digitalSignature* e *nonRepudiation* devem estar ativado;
"Extended Key Usage", crítica: somente o propósito *timeStamping OID* = 1.3.6.1.5.5.7.3.8 deve estar presente. nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil. Esse OID não deve ser empregado em qualquer outro tipo de

certificado;

d) para certificados de Assinatura A CF-e-SAT:
***"Key Usage"*, crítica**: deve conter o bit *digitalSignature* ativado, podendo conter os bits *keyAgreement* e *nonRepudiation* ativados;
***"Extended Key Usage", não crítica**:* somente o propósito *client authentication OID = 1.3.6.1.5.5.7.3.2* deve estar presente;

e) para certificados de Assinatura de Resposta OCSP:
***"Key Usage"*, crítica**: deve conter o bit *digitalSignature* ativado, podendo conter o bit *nonRepudiation* ativado;
***"Extended Key Usage"*, não crítica:** somente o propósito *OCSPSigning OID = 1.3.6.1.5.5.7.3.9* deve estar presente;

f) para os demais certificados de Assinatura e/ou Proteção de *e-Mail*:
***"Key Usage"*, crítica**: deve conter o bit *digitalSignature* ativado, podendo conter os bits *keyEncipherment* e *nonRepudiation* ativados;
***"Extended Key Usage", não crítica**:* no mínimo um dos propósitos *client authentication OID* = 1.3.6.1.5.5.7.3.2 ou *E-mail protection OID* = 1.3.6.1.5.5.7.3.4 deve estar ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos pelas AC, em suas PC, em conformidade com a RFC 5280; e

g) para certificados de Sigilo:
***"Key Usage"*, crítica**: somente os bits *keyEncipherment* e *dataEncipherment* podem estar ativados.

7.1.3 Identificadores de algoritmo

Neste item da PC deve ser indicado o OID (*Object Identifier)* do algoritmo criptográfico utilizado para assinatura do certificado, observados os algoritmos admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

7.1.4 Formatos de nome

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

C = BR

O = ICP-Brasil

OU = nome da AC emitente

OU = CNPJ da AR que realizou a identificação presencial

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ); em um certificado de equipamento ou aplicação, o identificador CN deverá conter o URL correspondente ou o nome da apli-

cação

7.1.4.2 O certificado digital emitido para equipamentos de carimbo do tempo de Autoridade de Carimbo do Tempo credenciada na ICP-Brasil deverá adotar o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = < nome da Autoridade de Carimbo do Tempo >

CN = < nome do Servidor de Carimbo do Tempo (incluindo o serial do SCT) >

7.1.4.3 O certificado digital emitido para assinatura de código deverá adotar o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

S = unidade da federação do endereço físico do titular do certificado
L = cidade do endereço físico do titular
Business Category **(OID 2.5.4.15)** = tipo de categoria comercial, devendo conter:
"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity"
SERIALNUMBER **(OID 2.5.4.5)** = CPF ou CNPJ, conforme o tipo de pessoa
Jurisdiction Country Name **(OID: 1.3.6.1.4.1.311.60.2.1.3)** = BR

7.1.4.4 O certificado digital emitido para autenticação de servidor (SSL/TLS) deverá adotar o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular

S = unidade da federação do endereço físico do titular do certificado
L = cidade do endereço físico do titular
Business Category **(OID 2.5.4.15)** = tipo de categoria comercial, devendo conter:
"Private Organization" ou "Government Entity" ou "Business Entity" ou "Non-Commercial Entity"

SERIALNUMBER (OID 2.5.4.5) = CPF ou CNPJ, conforme o tipo de pessoa
Jurisdiction Country Name **(OID: 1.3.6.1.4.1.311.60.2.1.3)** = BR

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5 Restrições de nome

7.1.5.1 Neste item da PC, devem ser descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2 A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e
b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

Tabela 7 - Caracteres especiais admitidos em nomes

Caractere	*Código NBR9611 (hexadecimal)*
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*****	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F

Caractere	*Código NBR9611 (hexadecimal)*
@	40
\	5C

7.1.6 OID (Object Identifier) da PC

Neste item, deve ser informado o OID atribuído à PC. Todo certificado emitido segundo a PC deverá conter, na extensão "*Certificate Policies*", o OID correspondente.

7.1.7 Uso da extensão "Policy Constraints"

Item não aplicável.

7.1.8 Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo a PC, o campo ***policyQualifiers*** da extensão "*Certificate Policies*" deverá conter o endereço *Web* (URL) da DPC da AC responsável.

7.1.9 Semântica de processamento para as extensões críticas de PC

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número de versão

As LCR geradas pela AC responsável, segundo a PC, deverão implementar a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 Neste item, a PC deve descrever todas as extensões de LCR utilizadas e sua criticalidade.

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

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

"*CRL Number*", não crítica: deve conter um número sequencial para cada LCR emitida.

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

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

7.3.2 Extensões de OCSP

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

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável, ou detalhados aspectos específicos para a PC, se houver.

8.1 Frequência e circunstâncias das avaliações

8.2 Identificação/Qualificação do avaliador

8.3 Relação do avaliador com a entidade avaliada

8.4 Tópicos cobertos pela avaliação

8.5 Ações tomadas como resultado de uma deficiência

8.6 Comunicação dos resultados

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens seguintes devem ser referidos os itens correspondentes da DPC da AC responsável, ou detalhados aspectos específicos para a PC, se houver. Os itens seguintes com requisitos especificados devem ser atendidos.

9.1 Tarifas

9.1.1 Tarifas de emissão e renovação de certificados

9.1.2 Tarifas de acesso ao certificado

9.1.3 Tarifas de revogação ou de acesso à informação de status

9.1.4 Tarifas para outros serviços

9.1.5 Política de reembolso

9.2 Responsabilidade Financeira

9.2.1 Cobertura do seguro

9.2.2 Outros ativos

9.2.3 Cobertura de seguros ou garantia para entidades finais

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.2 Informações fora do escopo de informações confidenciais

9.3.3 Responsabilidade em proteger a informação confidencial

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

9.4.2 Tratamento de informação como privadas

9.4.3 Informações não consideradas privadas

9.4.4 Responsabilidade para proteger a informação privadas

9.4.5 Aviso e consentimento para usar informações privadas

9.4.6 Divulgação em processo judicial ou administrativo

9.4.7 Outras circunstâncias de divulgação de informação

9.5 Direitos de Propriedade Intelectual

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

9.6.2 Declarações e Garantias da AR

9.6.3 Declarações e garantias do titular

9.6.4 Declarações e garantias das terceiras partes

9.6.5 Representações e garantias de outros participantes

9.7 Isenção de garantias

9.8 Limitações de responsabilidades

9.9 Indenizações

9.10 Prazo e Rescisão

9.10.1 Prazo

9.10.2 Término

9.10.3 Efeito da rescisão e sobrevivência

9.11 Avisos individuais e comunicações com os participantes

9.12 Alterações

9.12.1 Procedimento para emendas

Neste item devem ser descritos a política e os procedimentos utilizados para realizar alterações na PC. Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2 Mecanismo de notificação e períodos

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

9.12.3 Circunstâncias na qual o OID deve ser alterado

9.13 Solução de conflitos

9.14 Lei aplicável

9.15 Conformidade com a Lei aplicável

9.16 Disposições Diversas

9.16.1 Acordo completo

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

9.16.2 Cessão

9.16.3 Independência de disposições

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

9.17 Outras provisões

Toda PC deverá ser submetida à aprovação, durante o processo de credenciamento da AC responsável**,** conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Como parte desse processo, além da conformidade com este documento, deverá ser verificada a compatibilidade entre a PC e a DPC da AC responsável.

10 DOCUMENTOS REFERENCIADOS

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

Ref.	*Nome do documento*	*Código*
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**
[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DEPRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇADA ICP-BRASIL	**DOC-ICP-17**
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	**DOC-ICP-12**

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

Ref.	*Nome do documento*	*Código*
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	**DOC-ICP-01.01**
[2]	ATRIBUIÇÃO DE OID NA ICP-BRASIL	**DOC-ICP-04.01**

Anexo V

Infraestrutura de Chaves Públicas Brasileira

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

DOC-ICP-05

Versão 5.0

30 de maio de 2019

Sumário

Controle de alterações

Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
Resolução 151, de 30.05.2019 (Versão 5.0)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11	Atualização dos requisitos Webtrust e consolidação com a versão 4.7, com a simplificação dos processos da ICP-Brasil.
Resolução 139, de 03.07.2018 (Versão 4.6)	3.1.1.4.1, 3.1.1.11, 3.1.13, 4.4.2	Criação da Política de Certificado para Objetos Metrológicos – OM-BR no âmbito da ICP-Brasil.
Resolução 136, de 08.03.2018 (Versão 4.5)	3.1.10.1.3, 4.1.1.c	Aprovação dos procedimentos para criação do termo de titularidade.
Resolução 131, de 10.11.2017 (Versão 4.4)	3.1.1.10 e 3.1.9	Validação de solicitação de certificados para pessoas físicas titulares de contas de depósito.
Resolução 130, de 19.09.2017 (Versão 4.3)	3.1.1.2	Procedimentos de validação fora do ambiente físico da AR.
Resolução 119 e 121, de 06.07.2017 (Versão 4.2)	2.7.1 e 4.4.10 3.1.9.1, 4.1.1.alínea b, 4.1.1.alínea c, 4.4.2, 2.2.1.4	Obrigatoriedade de realização de auditorias WebTrust e de implementação de respostas OCSP para certificados do tipo SSL/TLS. Procedimentos para emissão de certificados digitais para servidores públicos da ativa e militares da União.
Resolução 118, de 09.12.2015 (Versão 4.1)	2.6.4 e 2.6.4.1	Define a obrigatoriedade da disponibilização de dois repositórios para a distribuição da LCR.
Resolução 115, de 11.11.2015 (Versão 4.0)	3.1.1.8, 3.1.11.1.4, 3.1.11.3.1 e 4.4.2.	Criação de Política de Certificado A CF-e-SAT.

Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
Resolução 114, de 30.09.2015 (Versão 3.9)	3.1.1.1, 3.1.1.7 (novo), 3.1.9, 3.1.9.1	Obrigatoriedade da coleta de dados biométricos do requerente do certificado digital.
Resolução 107, de 25.08.2015 (Versão 3.8)	3.1.1.1, alínea a, item i 3.2.2, alínea b	Limita o prazo de validade para até 90 dias nas procurações. Restringe a renovação automática não presencial apenas para pessoa física.
Resolução 99, de 09.10.2013 (Versão 3.7)	6.3.2.4	Amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolução 90, de 13.08.2012 (Versão 3.6)	3.1.9.1, 6.3.2.4	Inclui as Notas nº 5, 6 e 7 e altera a validade de certificados de AC.
Resolução 84, de 18.11.2010 (Versão 3.5)	2.2.1.3, 3.1.1.6, 3.1.9.1, 3.1.9.2.1, 4.1.1, 4.4.2	Inclui procedimentos para a emissão de certificados digitais que integram o documento de Registro de Identidade Civil-RIC.
Resolução n° 114, de 30.09.2015 (Versão 3.9)	3.1.1.1, 3.1.1.7 (novo), 3.1.9, 3.1.9.1	Obrigatoriedade da coleta de dados biométricos do requerente do certificado digital.
Resolução 107, de 25.08.2015 (Versão 3.8)	3.1.1.1, alínea a, item i 3.2.2, alínea b	Limita o prazo de validade para até 90 dias nas procurações. Restringe a renovação automática não presencial apenas para pessoa física.
Resolução 99, de 09.10.2013 (Versão 3.7)	6.3.2.4	Amplia prazo de validade de certificados das hierarquias da ICP-Brasil que implementam exclusivamente algoritmos de curvas elípticas.
Resolução 90, de 13.08.2012 (Versão 3.6)	3.1.9.1, 6.3.2.4	Inclui as Notas nº 5, 6 e 7 e altera a validade de certificados de AC.
Resolução 84, de 18.11.2010	2.2.1.3, 3.1.1.6, 3.1.9.1, 3.1.9.2.1,	Inclui procedimentos para a emissão de certificados digitais que integram o

Resolução que aprovou a alteração	Item Alterado	Descrição da Alteração
(Versão 3.5)	4.1.1, 4.4.2	documento de Registro de Identidade Civil-RIC.
Resolução 79, de 07.06.2010 (Versão 3.4)	3.1.1.1	Complementa os requisitos para procuração de pessoa jurídica, para aceitação apenas quando o ato constitutivo prevê.
Resolução 75, de 31.03.2010 (Versão 3.3)	4.6.2, 4.4.11	Altera prazo de retenção do dossiê.
Resolução 74, de 24.11.2009 (Versão 3.2)	2.1.3, 3.1.10.1.3, 3.1.10.3.2 4.1.1, 4.5.1.7, 9.3	Alterações relacionadas aos procedimentos operacionais para utilização de Termo de Titularidade.
Resolução 66, de 06.06.2009 (Versão 3.1)	3.2.2	Altera procedimentos para a renovação de certificados digitais de Pessoa Jurídica.
Resolução 54, de 19.11.2008 (Versão 3.0)	3.1.11.2.2 , 4.1.3	Inclusão de referências a Carimbo de Tempo.
Resolução 48, de 03.12.2007 (Versão 2.1)	3.1.10.2	Alterados os documentos a serem apresentados para identificação de uma organização que solicita certificado digital.
	3.1.1.5	Incluído item sobre identificação de Servidores do Serviço Exterior Brasileiro em missão permanente no exterior.
	6.6.4	Incluído item exigindo verificação de consistência do conteúdo das LCRs, antes de sua publicação.
Resolução 42, de 18.04.2006 (Versão 2.0)	Diversos	Criação do DOC-ICP-05, consolidando documentos anteriores.

1 INTRODUÇÃO

A ICP-Brasil é uma plataforma criptográfica de confiança. Garante presunção de validade jurídica aos atos e negócios eletrônicos assinados e cifrados com certificados digitais e chaves emitidos pelas entidades credenciadas na ICP-Brasil.

1.1 Visão Geral

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

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

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

1.1.4 A estrutura desta DPC está baseada na RFC 3647.

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

1.2 Nome do documento e identificação

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

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

a) autenticação de servidor (SSL/TLS);

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

c) assinatura de código (Code Signing); e

d) assinatura de carimbo do tempo (Timestamping).

1.3 Participantes da ICP-Brasil

1.3.1 Autoridades Certificadoras

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

1.3.2 Autoridades de Registro

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

certificados digitais e de identificação de seus solicitantes:

a) relação de todas as ARs credenciadas; e

b) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 Titulares do Certificado

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

1.3.4 Partes Confiáveis

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

1.3.5 Outros Participantes

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

1.4 Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

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

1.4.2 Uso proibitivo do certificado

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

1.5 Política de Administração

Neste item devem ser incluídos nome, endereço e outras informações da AC responsável pela DPC. Devem ser também informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC.

1.5.2 Contatos

Endereço:
Telefone:
Fax:
Página web:

E-mail:
Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome:
Telefone:
E-mail:
Outros:

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.
Os procedimentos de aprovação da DPC da AC são estabelecidos a critério do CG da ICP-Brasil.

1.6 Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	*Automatic Certificate Management Environment*
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*

LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
OM-BR	Objetos Metrológicos ICP-Brasil
OU	*Organization Unit*
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	*Proof of Possession*
PS	Política de Segurança
PSBio	Prestador de Serviço Biométrico
PSC	Prestador de Serviço de Confiança
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAT	Sistema Autenticador e Transmissor
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	*Simple Network Management Protocol*
SSL	*Secure Socket Layer*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 Repositórios

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

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

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

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

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

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

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

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

2.2 Publicação de informações dos certificados

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

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

a) seu próprio certificado;
b) suas LCRs/OCSP;
c) sua DPC;
d) as PCs que implementa;
e) uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços; e
f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3 Tempo ou Frequência de Publicação

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

2.4 Controle de Acesso aos Repositórios

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

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1 Atribuição de Nomes

3.1.1 Tipos de nomes

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

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

3.1.2 Necessidade dos nomes serem significativos

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

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4 Regras para interpretação de vários tipos de nomes

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

3.1.5 Unicidade de nomes

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

3.1.6 Procedimento para resolver disputa de nomes

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

estabelecer também que, durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

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

3.2 Validação inicial de identidade

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

a) Identificação do titular do certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.2.2, 3.2.3 e 3.2.7:

   i. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação e/ou biometria apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como a sua representante é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro dos 90 (noventa) dias anteriores à data da certificação. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim.

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

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

3.2.1 Método para comprovar a posse de chave privada

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

3.2.2 Autenticação da identificação da organização

3.2.2.1 Disposições Gerais

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

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

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

a) apresentação do rol de documentos elencados no item 3.2.2.2;
b) apresentação do rol de documentos elencados no item 3.2.3.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) presença física dos representantes legais, admitida a representação por procuração, conforme disposto no item 3.2, alínea 'a', inciso (i), e do responsável pelo uso do certificado; e
d) assinatura digital do termo de titularidade de que trata o item 4.1 pelo titular ou responsável pelo uso do certificado.

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

3.2.2.2 Documentos para efeitos de identificação de uma organização

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

a) Relativos a sua habilitação jurídica:
   i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
   ii. se entidade privada:
      1. ato constitutivo, devidamente registrado no órgão competente; e
      2. documentos da eleição de seus administradores, quando aplicável;
b) Relativos a sua habilitação fiscal:
   i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
   ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

3.2.2.3 Informações contidas no certificado emitido para uma organização

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

a) Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), sem abreviações;[1]
b) Cadastro Nacional de Pessoa Jurídica (CNPJ);[2]
c) Nome completo do responsável pelo certificado, sem abreviações;[3] e
d) Data de nascimento do responsável pelo certificado.[4]

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

3.2.3 Autenticação da identidade de um indivíduo

Neste item devem ser definidos os procedimentos empregados pelas AR vinculadas a uma AC para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo biométrico da ICP-Brasil.

3.2.3.1 Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original oficial, podendo ser física ou digital, por meio de barramento ou aplicação oficial, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado:

a) Registro de Identidade ou Passaporte, se brasileiro; ou

b) Título de Eleitor, com foto; ou

c) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil; ou

d) Passaporte, se estrangeiro não domiciliado no Brasil;

e) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11]; e

f) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

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

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

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

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

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

a) por agente de registro distinto do que realizou a etapa de identificação;
b) na sede da AR ou AR própria da AC; e
c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

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

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

3.2.3.1.6 É facultado aos Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo BACEN, na identificação de titulares pessoa física de conta de depósito, e as serventias extrajudiciais autorizadas a funcionar pelo Conselho Nacional de Justiça, utilizar o recurso disposto no item 3.2.9.4.

3.2.3.2 Informações contidas no certificado emitido para um indivíduo

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

a) nome completo, sem abreviações; [1]
b) data de nascimento.[2]

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

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

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

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

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

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

3.2.4 Informações não verificadas do titular do certificado

Não se aplica.

3.2.5 Validação das autoridades

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

3.2.6 Critérios para interoperação

Não se aplica.

3.2.7 Autenticação da identidade de equipamento ou aplicação

3.2.7.1 Disposições Gerais

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

3.2.7.1.2 Se o titular for pessoa física, deverá ser feita a confirmação de sua identidade na forma do item 3.2.3.1 e esta assinará o termo de titularidade de que trata o item 4.1.

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

a) Apresentação do rol de documentos elencados no item 3.2.2.2;
b) Apresentação do rol de documentos elencados no item 3.2.3.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
c) Presença física do responsável pelo uso do certificado e assinatura do termo de titularidade e responsabilidade de que trata o item 4.1; e
d) Presença física do(s) representante(s) legal(is) da pessoa jurídica e assinatura do termo de titularidade e responsabilidade de que trata o item 4.1, ou outorga de procuração atribuindo poderes para solicitação de certificado para equipamento ou aplicação e assinatura do respectivo termo de titularidade.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

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

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

3.2.7.3 Informações contidas no certificado emitido para um equipamento ou aplicação

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

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

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

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

3.2.7.4.1 Disposições Gerais

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

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

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

3.2.7.5 Procedimentos para efeitos de identificação de um equipamento SAT

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

3.2.7.6 Informações contidas no certificado emitido para um equipamento SAT

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

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

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

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

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

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

3.2.7.7 Autenticação de identificação de equipamentos para certificado OM-BR

3.2.7.7.1 Disposições gerais

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

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

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

3.2.7.8 Procedimentos para efeitos de identificação de um equipamento metrológico

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

3.2.7.9 Informações contidas no certificado emitido para um equipamento metrológico

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

a) data de fabricação do equipamento metrológico;
b) número de identificação do equipamento metrológico;
c) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;
d) Cadastro Nacional de Pessoa Jurídica (CNPJ).

---

1 No campo *Subject*, como parte do *Common Name,* que compõe o *Distinguished Name*

2 No campo *Subject Alternative Name, OID* ***2.16.76.1.3.8***

3 No campo *Subject Alternative Name,* OID **2.16.76.1.3.3**

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

3.2.8 Procedimentos complementares

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

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

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

3.2.8.3.1 No caso de certificados A CF-e-SAT ou OM-BR deve ser mantida toda a documentação eletrônica utilizada no processo de validação e confirmação da identificação do equipamento SAT ou objeto metrológico acreditado pelo Inmetro, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.2.8.4 As AC devem disponibilizar, para todas as AR vinculadas a sua respectiva cadeia, uma interface para verificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, conforme estabelecido no DOC-ICP-03 [6] e DOC-ICP-05.02 [10].

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

3.2.9 Procedimentos específicos

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

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

a) validar o registro inicial por meio de verificação da assinatura digital do contribuinte realizada

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

b) realizar a verificação da solicitação, assinada digitalmente, contendo a requisição em conformidade com o formato estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] e confrontando com as informações (número de segurança e número de série do equipamento SAT e CNPJ do contribuinte emissor CF-e) do registro inicial e do certificado digital que assinou esse registro inicial;

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

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

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

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

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

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

3.2.9.3.1 Módulo Eletrônico da AR dos Órgãos Gestores de Pessoas

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

a) ser um sistema vinculado a uma AC credenciada pela ICP-Brasil, de acordo com esta Instrução Normativa;

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

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

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

e) possuir as listas atualizadas com os nomes e CPF ou outro indexador dos servidores

públicos, dos militares e dos autorizadores, com a comprovação auditável da resposta do sistema biométrico do Tribunal Superior Eleitoral ou prestadores de serviço biométrico da ICP-Brasil ou pelo custodiante de outra base biométrica oficial. Os autorizadores serão formalmente designados pelos órgãos competentes, por instrumento normativo.

Nota: Ficam excepcionalizados para as AR descritas no item 3.2.9.3.1 os requisitos dispostos no DOC-ICP-03.01[1].

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

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

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

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

3.2.9.4 A AR de Bancos Múltiplos ou Caixa Econômica Federal e as serventias extrajudiciais credenciada na ICP-Brasil deverá ter um módulo eletrônico de AR.

3.2.9.4.1 A AR, representada pelo módulo eletrônico, deverá:

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

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

c) comunicar diretamente utilizando protocolos de comunicação seguro com os sistemas determinados formalmente pelos Bancos Múltiplos e Caixa Econômica Federal e das as serventias extrajudiciais, pela AR (quando aplicável), pela AC e pelo Prestador de Serviço Biométrico (PSBIO);

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

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

Nota: As AR descritas no item 3.2.9.4 ficam dispensadas dos requisitos dispostos no item "Segurança de Pessoal" e no item "Aplicativo de AR" do DOC-ICP-03.01, para aqueles requisitos equivalentes aos previstos nas normas do Banco Central do Brasil e Conselho Nacional de Justiça.

3.2.9.5 Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR:

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

a) validar o registro inicial por meio de verificação da assinatura digital do fabricante do

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

b) realizar a verificação da solicitação, assinada digitalmente, contendo a requisição em conformidade com o formato estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] e confrontando com as informações de controle do órgão regulador e do certificado digital que assinou a requisição;

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

3.3 Identificação e autenticação para pedidos de novas chaves

3.3.1 Identificação e autenticação para rotina de novas chaves antes da expiração

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

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

a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;

b) a solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva, permitida tal hipótese apenas para os certificados digitais de pessoa física;

c) por meio de mecanismo automatizado de gerenciamento de certificado do tipo SSL/TLS (ACME), conforme disposto no item 3.3.1.2.1.

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

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

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

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

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

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

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

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

3.3.2 Identificação e autenticação para novas chaves após a revogação

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

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

3.4 Identificação e Autenticação para solicitação de revogação

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

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

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 Solicitação do certificado

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

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

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

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

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

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

4.1.1 Quem pode submeter uma solicitação de certificado

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

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

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

4.1.1.3 Nos casos previstos no item 4.1.1.1, a AC subsequente deverá encaminhar a solicitação de certificado à AC emitente por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

4.1.2 Processo de registro e responsabilidades

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

4.1.2.1 Responsabilidades da AC

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

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

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

4.1.2.2 Obrigações da AC

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

a) operar de acordo com a sua DPC e com as PCs que implementa;
b) gerar e gerenciar os seus pares de chaves criptográficas;
c) assegurar a proteção de suas chaves privadas;
d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) distribuir o seu próprio certificado;
g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente ao seu ou os certificados de AR a ela vinculadas e de usuários finais;
h) informar a emissão do certificado ao respectivo solicitante;
i) revogar os certificados por ela emitidos;
j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
k) publicar em sua página *web* sua DPC e as PCs aprovadas que implementa;
l) publicar, em sua página *web,* as informações definidas no item 2.2.2 deste documento;
m) publicar, em página web, informações sobre o descredenciamento de AR;
n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;
o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do CG da ICP-Brasil;
u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;

v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços; e
y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados.

4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4 Obrigações das ARs

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

a) receber solicitações de emissão ou de revogação de certificados;
b) confirmar a identidade do solicitante e a validade da solicitação;
c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1];
d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1], bem como Princípios e Critérios WebTrust para AR [5];
f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.2.2, 3.2.3 e 3.2.7; e
h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios WebTrust para AR [5].

4.2 Processamento de Solicitação de Certificado

4.2.1 Execução das funções de identificação e autenticação

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

4.2.2 Aprovação ou rejeição de pedidos de certificado

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

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

4.2.3 Tempo para processar a solicitação de certificado

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

4.3 Emissão de Certificado

4.3.1 Ações da AC durante a emissão de um certificado

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

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

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

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

4.4 Aceitação de Certificado

4.4.1 Conduta sobre a aceitação do certificado

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

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

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

4.4.2 Publicação do certificado pela AC

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

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

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

4.5 Usabilidade do par de chaves e do certificado

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

4.5.1 Usabilidade da Chave privada e do certificado do titular

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

4.5.1.2 Obrigações do Titular do Certificado

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

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil; e
e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

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

4.5.2 Usabilidade da chave pública e do certificado das partes confiáveis

Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Em acordo com item 3.3 desta DPC.

4.6.1 Circunstâncias para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.2 Quem pode solicitar a renovação

Em acordo com item 3.3 desta DPC.

4.6.3 Processamento de requisição para renovação de certificados

Em acordo com item 3.3 desta DPC.

4.6.4 Notificação para nova emissão de certificado para o titular

Em acordo com item 3.3 desta DPC.

4.6.5 Conduta constituindo a aceitação de uma renovação de um certificado

Em acordo com item 3.3 desta DPC.

4.6.6 Publicação de uma renovação de um certificado pela AC

Não se aplica.

4.6.7 Notificação de emissão de certificado pela AC para outras entidades

Em acordo com item 4.3 desta DPC.

4.7 Nova chave de certificado (Re-key)

4.7.1 Circunstâncias para nova chave de certificado

Não se aplica

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

Não se aplica

4.7.3 Processamento de requisição de novas chaves de certificado

Não se aplica

4.7.4 Notificação de emissão de novo certificado para o titular

Não se aplica

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica

4.7.6 Publicação de uma nova chave certificada pela AC

Não se aplica

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

Não se aplica

4.8 Modificação de certificado

Não se aplica

4.8.1 Circunstâncias para modificação de certificado

Não se aplica

4.8.2 Quem pode requisitar a modificação de certificado

Não se aplica

4.8.3 Processamento de requisição de modificação de certificado

Não se aplica

4.8.4 Notificação de emissão de novo certificado para o titular

Não se aplica

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica

4.8.6 Publicação de uma modificação de certificado pela AC

Não se aplica

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

Não se aplica

4.9 Suspensão e Revogação de Certificado

4.9.1 Circunstâncias para revogação

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

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

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

4.9.1.3 A DPC deve observar ainda que:

a) A AC emitente deverá revogar, no prazo definido no item 4.9.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
b) O CG da ICP-Brasil ou a AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

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

4.9.1.4.1 ACs que emitem certificados SSL e CS devem suportar requisições OCSP em conformidade

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

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

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

4.9.2 Quem pode solicitar revogação

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

a) Por solicitação do titular do certificado;
b) Por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
c) Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
d) Pela AC emitente;
e) Por uma AR vinculada;
f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
g) Pela unidade fiscal federada do contribuinte, quando tratar-se de certificado do tipo A CF-e-SAT;
h) Por servidores públicos da ativa e militares da União, Estados e Distrito Federal autorizados pelos respectivos órgãos competentes pela identificação dos mesmos;
i) Pelo Inmetro, quando se tratar de certificado do tipo OM-BR.

4.9.3 Procedimento para solicitação de revogação.

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

4.9.3.2 Como diretrizes gerais, a DPC deve estabelecer que:

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

4.9.3.3 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de

12 (doze) horas.

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

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

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

4.9.4 Prazo para solicitação de revogação

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

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

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

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

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

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

4.9.7 Frequência de emissão de LCR

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

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

4.9.7.3 A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC responsável deverá emitir nova LCR no prazo previsto no item 4.9.3.4 e notificar todas as ACs de nível imediatamente subsequente ao seu.

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

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

4.9.8 Latência máxima para a LCR

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

4.9.9 Disponibilidade para revogação/verificação de status on-line

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

4.9.10 Requisitos para verificação de revogação on-line

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

4.9.11 Outras formas disponíveis para divulgação de revogação

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

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

4.9.12 Requisitos especiais para o caso de comprometimento de chave

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

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

4.9.13 Circunstâncias para suspensão

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

4.9.14 Quem pode solicitar suspensão

A AC, aprovados pelo Comitê Gestor.

4.9.15 Procedimento para solicitação de suspensão

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

4.9.16 Limites no período de suspensão

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

4.10 Serviços de status de certificado

4.10.1 Características operacionais

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

4.10.2 Disponibilidade dos serviços

Ver item 4.9

4.10.3 Funcionalidades operacionais

Ver item 4.9

4.11 Encerramento de atividades

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

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

4.12 Custódia e recuperação de chave

4.12.1 Política e práticas de custódia e recuperação de chave

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

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

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

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

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

5.1 Controles físicos

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

5.1.1 Construção e localização das instalações de AC

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

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

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

5.1.2 Acesso físico

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

5.1.2.1 Níveis de acesso

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

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

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

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

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

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

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

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

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

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

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

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

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

ou superior.

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

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

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

5.1.2.2 Sistemas físicos de detecção

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

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

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

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

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

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

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1 Mecanismos específicos deverão ser implantados pela AC para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos deverão permitir o

destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos deve acionar imediatamente os alarmes de abertura de portas.

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

5.1.3 Energia e ar-condicionado

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

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

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

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

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

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

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

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

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

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

a) Geradores de porte compatível;
b) Geradores de reserva;
c) Sistemas de *no-breaks* redundantes; e
d) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

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

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

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

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

5.1.6 Armazenamento de mídia

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

5.1.7 Destruição de lixo

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

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

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

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

5.2 Controles Procedimentais

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

também ser estabelecido o número de pessoas requerido para sua execução.

5.2.1 Perfis qualificados

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

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

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

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

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

5.2.2 Número de pessoas necessário por tarefa

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

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

5.2.3 Identificação e autenticação para cada perfil

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

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

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

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

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

5.2.4 Funções que requerem separação de deveres

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

5.3 Controles de Pessoal

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

a) Os termos e as condições do perfil que ocuparão;
b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e
c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

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

5.3.2 Procedimentos de verificação de antecedentes

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

a) Verificação de antecedentes criminais;
b) Verificação de situação de crédito;
c) Verificação de histórico de empregos anteriores; e
d) Comprovação de escolaridade e de residência.

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

5.3.3 Requisitos de treinamento

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

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

b) Sistema de certificação em uso na AC;

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

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

e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

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

5.3.5 Frequência e sequência de rodízio de cargos

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

5.3.6 Sanções para ações não autorizadas

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

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

a) Relato da ocorrência com "*modus operandis*";
b) Identificação dos envolvidos;
c) Eventuais prejuízos causados;
d) Punições aplicadas, se for o caso; e
e) Conclusões.

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

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

a) Advertência;
b) Suspensão por prazo determinado; ou
c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para contratação de pessoal

Todo o pessoal da AC responsável e das ARs vinculadas envolvido em atividades diretamente

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

5.3.8 Documentação fornecida ao pessoal

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

a) Sua DPC;

b) As PCs que implementa;

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

d) Documentação operacional relativa a suas atividades; e

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

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

5.4 Procedimentos de Log de Auditoria

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

5.4.1 Tipos de eventos registrados

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

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
c) Mudanças na configuração da AC ou nas suas chaves;
d) Mudanças nas políticas de criação de certificados;
e) Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
f) Tentativas não-autorizadas de acesso aos arquivos de sistema;
g) Geração de chaves próprias da AC ou de chaves de seus usuários finais;
h) Emissão e revogação de certificados;
i) Geração de LCR;
j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
l) Operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1 A AC, emissora de certificados SSL e CS, deve ter capacidade de auditar esses tipos

certificados em até seis por cento dos emitidos.

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

a) Registros de acessos físicos;
b) Manutenção e mudanças na configuração de seus sistemas;
c) Mudanças de pessoal e de perfis qualificados;
d) Relatórios de discrepância e comprometimento; e
e) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

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

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

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

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

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

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

5.4.2 Frequência de auditoria de registros

A DPC deve estabelecer a periodicidade, não superior a uma semana, com que os registros de auditoria da AC responsável serão analisados pelo seu pessoal operacional. Todos os eventos significativos deverão ser explicados em relatório de auditoria de registros. Tal análise deverá envolver uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise deverão ser documentadas.

5.4.3 Período de retenção para registros de auditoria

Neste item, a DPC deve estabelecer que a AC responsável manterá localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, deverá armazená-los da maneira descrita no item 5.5.

5.4.4 Proteção de registros de auditoria

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

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

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

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

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

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

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

5.4.7 Notificação de agentes causadores de eventos

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

5.4.8 Avaliações de vulnerabilidade

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

5.5 Arquivamento de Registros

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

5.5.1 Tipos de registros arquivados

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

a) Solicitações de certificados;
b) Solicitações de revogação de certificados;
c) Notificações de comprometimento de chaves privadas;
d) Emissões e revogações de certificados;

e) Emissões de LCR;
f) Trocas de chaves criptográficas da AC responsável; e
g) Informações de auditoria previstas no item 5.4.1.

5.5.2 Período de retenção para arquivo

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

a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
b) Os dossiês dos titulares devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.

5.5.3 Proteção de arquivo

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

5.5.4 Procedimentos de cópia de arquivo

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

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

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

5.5.5 Requisitos para datação de registros

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

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

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

5.5.7 Procedimentos para obter e verificar informação de arquivo

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

5.6 Troca de chave

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

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

5.7 Comprometimento e Recuperação de Desastre

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

5.7.1 Procedimentos gerenciamento de incidente e comprometimento

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

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

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

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

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

d) Documentação dos processos e procedimentos acordados;

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

f) Teste e atualização dos planos.

5.7.2 Recursos computacionais, software, e/ou dados corrompidos

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

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

Neste item da DPC devem ser descritos os procedimentos de recuperação utilizados na circunstância

de revogação do certificado da AC responsável.

5.7.3.2 Chave de entidade é comprometida

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

5.7.4 Capacidade de continuidade de negócio após desastre

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

5.8 Extinção da AC

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

6 CONTROLES TÉCNICOS DE SEGURANÇA

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

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

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

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

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

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

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

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

6.1.2 Entrega da chave privada à entidade

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

6.1.3 Entrega da chave pública para emissor de certificado

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

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

6.1.4 Entrega de chave pública da AC às terceiras partes

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

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

6.1.5 Tamanhos de chave

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

6.1.5.2 Caso a AC responsável emita certificados para outras ACs, neste item deve ser também informado o tamanho das chaves criptográficas associadas a esses certificados, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

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

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

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

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

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

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

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

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

6.2.1 Padrões e controle para módulo criptográfico

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

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

6.2.2 Controle "n de m" para chave privada

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

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

6.2.3 Custódia (escrow) de chave privada

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

controles de segurança do sistema de recuperação.

6.2.4 Cópia de segurança de chave privada

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

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

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

6.2.4.4 Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

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

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

6.2.6 Inserção de chave privada em módulo criptográfico

Neste item da DPC, quando aplicáveis, devem ser definidos os requisitos para inserção da chave privada da AC responsável em módulo criptográfico. A RFC 4210 e 6712 poderá ser utilizada para esse fim. Cada PC implementada deve definir, quando aplicáveis, os requisitos para inserção da chave privada dos titulares de certificado em módulo criptográfico.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8 Método de ativação de chave privada

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

6.2.9 Método de desativação de chave privada

Neste item da DPC devem ser descritos os requisitos e os procedimentos necessários para desativação da chave privada da AC responsável. Devem ser definidos os agentes autorizados, o método de

confirmação da identidade desses agentes e as ações necessárias. Cada PC implementada deve descrever os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10 Método de destruição de chave privada

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

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

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

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

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

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

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

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

6.4 Dados de Ativação

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

6.4.1 Geração e instalação dos dados de ativação

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

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

6.4.2 Proteção dos dados de ativação

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

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

6.4.3 Outros aspectos dos dados de ativação

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

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

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

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

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

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

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

6.5.1.5 Qualquer equipamento, ou parte deste, ao ser enviado para manutenção deverá ter apagadas as

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

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

6.5.2 Classificação da segurança computacional

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

6.5.3 Controles de Segurança para as Autoridades de Registro

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

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

6.6 Controles Técnicos do Ciclo de Vida

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

6.6.1 Controles de desenvolvimento de sistema

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

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

6.6.2 Controles de gerenciamento de segurança

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

6.6.2.2 Uma metodologia formal de gerenciamento de configuração deverá ser usada para a instalação

e a contínua manutenção do sistema de certificação da AC.

6.6.3 Controles de segurança de ciclo de vida

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

6.6.4 Controles na Geração de LCR

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

6.7 Controles de Segurança de Rede

6.7.1 Diretrizes Gerais

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

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

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

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

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

6.7.2 *Firewall*

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

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

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O sistema de detecção de intrusão deverá ter capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps SNMP*,

executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

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

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

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – deverão ser registradas em arquivos para posterior análise, que poderá ser automatizada. A frequência de exame dos arquivos de registro deverá ser, no mínimo, diária e todas as ações tomadas em decorrência desse exame deverão ser documentadas.

6.8 Carimbo de Tempo

Em acordo com os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL[12].

7 PERFIS DE CERTIFICADO, LCR E OCSP

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC responsável deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280. O conteúdo e perfis dos certificados emitidos nas cadeias EV SSL e EV CS devem seguir os estabelecidos nos documentos EV SSL e EV CS Guidelines.

7.1.1 Número de versão

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

7.1.2 Extensões de certificado

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

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

d.1) o campo policyIdentifier deve conter:

i. o OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs; ou
ii. os OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;

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

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

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

7.1.3 Identificadores de algoritmo

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

7.1.4 Formatos de nome

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

C = BR

O = ICP-Brasil

OU = nome da AC emitente

CN = nome da AC titular

7.1.5 Restrições de nome

Neste item da DPC, devem ser descritas as restrições aplicáveis para os nomes de AC titulares de certificados, em conformidade com as restrições gerais estabelecidas pela ICP-Brasil no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

7.1.6 OID (Object Identifier) da DPC

Neste item, deve ser informado o OID da DPC.

7.1.7 Uso da extensão "Policy Constraints"

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

7.1.8 Sintaxe e semântica dos qualificadores de política

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

7.1.9 Semântica de processamento para as extensões críticas de PC

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

7.2.1 Número(s) de versão

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

7.2.2 Extensões de LCR e de suas entradas

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

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

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

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

7.3 Perfil de OCSP

7.3.1 Número(s) de versão

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

7.3.2 Extensões de OCSP

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

8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1 Frequência e circunstâncias das avaliações

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

8.2 Identificação/Qualificação do avaliador

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

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

ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

8.3 Relação do avaliador com a entidade avaliada

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

8.4 Tópicos cobertos pela avaliação

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

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

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

8.5 Ações tomadas como resultado de uma deficiência

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

8.6 Comunicação dos resultados

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

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 Tarifas

9.1.1 Tarifas de emissão e renovação de certificados

As tarifas de emissão e de renovação de certificado pela AC Raiz estão definidas no documento

DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

9.1.2 Tarifas de acesso ao certificado

Não se aplica.

9.1.3 Tarifas de revogação ou de acesso à informação de status

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

9.1.4 Tarifas para outros serviços

Tarifas para outros serviços da AC Raiz estão definidas no documento DIRETRIZES DA POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [13].

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

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

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

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

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

9.3.2 Informações fora do escopo de informações confidenciais

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

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

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

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

a) qualquer PC aplicável;

b) qualquer DPC;

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

d) a conclusão dos relatórios da auditoria.

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

9.3.3 Responsabilidade em proteger a informação confidencial

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

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

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

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

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

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

9.4.2 Tratamento de informação como privadas

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

9.4.3 Informações não consideradas privadas

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

9.4.4 Responsabilidade para proteger a informação privadas

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

9.4.5 Aviso e consentimento para usar informações privadas

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

O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.
Autorizações formais podem ser apresentadas de duas formas:

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

9.4.6 Divulgação em processo judicial ou administrativo

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

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

9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8 Informações a terceiros

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

9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

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

9.6.1.2 Precisão da informação

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

9.6.1.3 Identificação do requerente

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

9.6.1.4 Consentimento dos titulares

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

9.6.1.5 Serviço

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

9.6.1.6 Revogação

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

9.6.1.7 Existência Legal

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

9.6.2 Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

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

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

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1 As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
b) verificar, a qualquer tempo, a validade do certificado.

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

i. tiver sido emitido pela AC;
ii. não constar como revogado pela AC;
iii. não estiver expirado; e
iv. puder ser verificado com o uso do certificado válido da AC.

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

9.6.5 Representações e garantias de outros participantes

Não se aplica.

9.7 Isenção de garantias

Não se aplica.

9.8 Limitações de responsabilidades

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

9.9 Indenizações

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

9.10 Prazo e Rescisão

9.10.1 Prazo

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

9.10.2 Término

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

9.10.3 Efeito da rescisão e sobrevivência

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

9.11 Avisos individuais e comunicações com os participantes

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

9.12 Alterações

9.12.1 Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida para AC Raiz.

9.12.2 Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no site da AC.

9.12.3 Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13 Solução de conflitos

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

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

9.14 Lei aplicável

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

9.15 Conformidade com a Lei aplicável

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

9.16 Disposições Diversas

9.16.1 Acordo completo

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

9.16.2 Cessão

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

9.16.3 Independência de disposições

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

9.16.4 Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17 Outras provisões

Não se aplica.

10 DOCUMENTOS REFERENCIADOS

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

Ref.	*Nome do documento*	*Código*
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-09**
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-08**
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE PRESTADOR DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL	**DOC-ICP-17**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	**DOC-ICP-04**
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	**DOC-ICP-02**
[12]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	**DOC-ICP-12**
[13]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	**DOC-ICP-06**

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

Ref.	*Nome do documento*	*Código*
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL	**DOC-ICP-03.01**
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	**DOC-ICP-01.01**
[10]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE	**DOC-ICP-05.02**

Ref.	*Nome do documento*	*Código*
	IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL	
[11]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	**DOC-ICP-05.03**

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

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

11 REFERÊNCIAS BIBLIOGRÁFICAS

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

Anexo VI

Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL

DOC-ICP-05.02

Versão 2.0

30 de maio de 2019

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 151 de 30.05.2019 (Versão 2.0)	1, 2, 3, e 4	Simplificação dos Processos da ICP-Brasil.
Instrução Normativa nº 04, de 30.04.2019 (Versão 1.8)	2.2.6	Trata da solicitação de certificado para servidores públicos federais da ativa e militares da união.
Resolução 141 de 03.07.2018 (Versão 1.7)	2.2.6.2	Incluir os servidores públicos dos estados e do Distrito Federal nos procedimentos específicos de emissão de certificados digitais.
Resolução nº 131, de 10.11.2017 (Versão 1.6)	2.2.1, 2.2.3 e 2.2.7	Identificação de titulares de contas de depósito e validade da CNH.
Resolução nº 128, de 13.09.2017 (Versão 1.5)	2.2.1.c	Esclarece a obrigatoriedade de validação das informações contidas no *Subject Alternative Name*.
Instrução Normativa nº 06, de 11.08.2017 (Versão 1.4)	2.2.6, Nota 15-A (novos)	Validação de solicitação de certificados para servidores públicos da ativa e militares da União.
Instrução Normativa nº 01, de 31.03.2016 (Versão 1.3)	2.2.5.6, Nota 16 e Nota 17	Especificações para upload de imagens.
Instrução Normativa nº 08, de 10.12.2015 (Versão 1.2)	1.2, 2.1.1, 2.2, 2.2.1 e 2.2.5 (novo) e 2.2.5.9	Altera o termo titular do certificado digital por requerente do certificado digital.
Instrução Normativa nº 04, de 25.08.2015 (Versão 1.1)	Item 2.1.1.a	Estabelece prazo de validade de 90 (noventa) dias às procurações públicas de representantes de Pessoa Jurídica e determina o comparecimento presencial destes, vedada qualquer espécie de procuração para tal fim.
Instrução Normativa nº 02, de 23.06.2015 (Versão 1.0)	Novo documento	Cria a versão 1.0 do Documento Procedimentos para Identificação do Requerente e Comunicação de Irregularidades no Processo de Emissão de um Certificado Digital ICP-Brasil .

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridade de Registro
AGR	Agente de Registro
CNAE	Classificação Nacional de Atividades Econômicas
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro Nacional de Pessoa Física
CTPS	Carteira de Trabalho e Previdência Social
DPC	Declarações de Práticas de Certificação
IBGE	Instituto Brasileiro de Geografia e Estatística
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
PIS/PASEP	Programa de Integração Social/Programa de Formação do Patrimônio do Servidor Público
RG	Registro Geral
UF	Unidade Federativa

1 DISPOSIÇÕES GERAIS

1.1 Este documento se aplica ao processo de identificação do requerente de certificado digital, bem como das comunicações de eventuais tentativas de fraudes e irregularidades na emissão de um certificado digital ICP-Brasil.

1.2 Para o presente documento, aplicam-se os seguintes conceitos:

a) Agente de registro (AGR) – Pessoa responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a identificação do requerente quando da solicitação de certificados.

b) Autoridade de registro – AR - Entidade responsável pela interface entre o usuário e a Autoridade Certificadora – AC. É sempre vinculada a uma AC e tem por objetivo o recebimento e encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes.

c) Confirmação da identidade de um indivíduo – Comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada.

d) Confirmação da identidade de uma organização – Comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição.

e) Emissão do certificado – Conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.

f) identificação do requerente de certificado – Compreende na etapa de confirmação da identidade de um individuo ou de uma organização, realizadas mediante a presença física do interessado, com base nos documentos de identificação e/ou identificação biométrica, e a etapa de emissão do certificado.

g) Ponto de Centralização da AC – Local único, em território nacional, onde a AC armazena os dossiês de todos os Agentes de Registro das AR vinculadas. Deve armazenar os dossiês eletrônicos de titulares de certificados da ICP-Brasil e deve armazenar eletronicamente os documentos de identificação, fotografia da face e impressões digitais do requerente.

h) Lista Negativa – Conjunto de informações derivadas dos comunicados de fraude, ou indícios de fraude, feitos pelas AC (ou pelo próprio ITI por meio de

auditoria/fiscalização) da ICP-Brasil ao ITI, em que contém o modo de operação da ocorrência, as informações biográficas do documento apresentado e, se for o caso, das informações sobre a empresa, características fisiológicas do suposto fraudador, a imagem da face e do documento de identificação utilizado pelo suposto fraudador.

i) Sistema Biométrico ICP-Brasil – Sistema composto pelos Prestadores de Serviço Biométrico - PSBio, credenciados pelo ITI, responsáveis pela identificação (1:N) biométrica (que formará um registro/requerente único em um ou mais bancos/sistemas de dados biométrico para toda ICP-Brasil), bem como pela verificação (1:1) biométrica do requerente de um certificado digital (que trata da comparação entre uma biometria, que possua característica perene e unívoca, de acordo com os padrões internacionais de uso, como, por exemplo, impressão digital, face, íris, voz, coletada no processo de emissão do certificado digital com outra já armazenada em bancos/sistemas de dados biométrico da ICP-Brasil relativa ao mesmo requerente registro/indexador).

2 VERIFICAÇÃO DA IDENTIDADE DO REQUERENTE

2.1 Conforme estabelecido no DOC-ICP-05 [1], as AC definem em suas DPC os procedimentos empregados pelas suas AR vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e/ou pelo processo de identificação biométrica ICP-Brasil.

2.2 Caso o interessado, pessoa física, já tenha dossiê identificado pela AR, não será necessário nova apresentação dos documentos, exceto quando houver alteração de dados ou a necessidade de complementar a documentação.

2.3 Os resultados, sem irregularidades, da consulta/validação da identificação do requerente de um certificado deverão ser apensados ao dossiê eletrônico do titular.

2.4 As AC devem possuir uma interface para consulta a base de dados da Lista Negativa das ACs, com requisitos de segurança e disponibilidade, nos processos de conferência do documento em papel de emissão de um certificado digital ICP-Brasil.

2.4.1 Essa base de dados da Lista Negativa da AC deve ser atualizada pela comunicação entre o servidor da AC e o servidor do ITI, conforme disposto no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa).

2.4.2 Caso a AR e/ou a AC concluam pela não emissão do certificado digital, a AR, se for o caso, deve comunicar a AC, e essa deve comunicar a tentativa de fraude ao ITI, conforme disposto do item 3. Caso a AR e/ou a AC concluam pela emissão do certificado digital, a AC deve solicitar o cancelamento de fraude, ou tentativa, na Lista Negativa, embasando detalhadamente os motivos de tal, conforme disposto no item 3.

2.5 As AC devem disponibilizar, para todas as AR vinculadas à sua respectiva cadeia, uma interface para verificação e identificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil, em cada processo de emissão de um certificado digital ICP-Brasil, podendo ser coletada ou verificada a biometria uma única vez para o mesmo titular de vários certificados no ato presencial de identificação.

2.5.1 O Prestador de Serviço Biométrico – PSBio – da ICP-Brasil, que proverá os componentes do sistema biométrico, deve operar e ser credenciado, auditado e fiscalizado, conforme o disposto nos DOC-ICP-05.03 [6], DOC-ICP-03 [2], DOC-ICP-08 [3] e DOC-ICP-09 [4].

2.5.2 A interface da aplicação para os AGR deve disponibilizar, no mínimo, uma consulta pelo CPF (indexador) do requerente do certificado digital, com a coleta de uma biometria (por exemplo, uma impressão digital – preferencialmente a que possui melhor qualidade – e/ou face) do mesmo no processo de emissão do certificado digital, que deve ser enviada/comparada obrigatoriamente com o registro daquela biometria específica do requerente em um banco/sistema de dados biométricos credenciado da ICP-Brasil. Caso o CPF (indexador) esteja no banco/sistema de dados biométricos da ICP-Brasil, a consulta deve indicar um resultado "positivo" (biometria comparada pertence de fato ao requerente, apresentando também, no mínimo, a face e o nome do requerente para o AGR), ou "negativo" (biometria comparada não pertence ao requerente ou resultou em um erro). Caso o CPF (indexador) não conste na base de dados biométrica da ICP-Brasil, tal fato deve ser informado ao AGR.

2.5.3 O resultado "positivo" da consulta à base de dados biométrica da ICP-Brasil deve ser apensado ao dossiê do titular do certificado e preservados de acordo com o DOC-ICP-03.01 [7].

NOTA 1: Todos os logs de transação biométrica feitos pelo AGR devem ser guardados pelo período de 7 anos pelas AC, conforme disposto no DOC-ICP-05 [1].

NOTA 2: Devem ser coletadas as informações biográficas e biométricas, esta última conforme DOC-ICP-05.03 [6] a serem enviadas para AC e, posteriormente enviados ao PSBio.

NOTA 3: Um Sistema Biométrico da ICP-Brasil credenciado deve reportar aos outros sistemas biométricos da ICP-Brasil credenciados, se for o caso, e às AC qualquer irregularidade ou duplicidade relativa ao armazenamento biométrico/biográfico de um registro detectada no processo de emissão de um certificado digital, para que as AC solicitantes do cadastro irregular providenciem, se for o caso, a revogação do certificado digital e a comunicação de eventual fraude.

2.5.4 Caso o resultado da verificação biométrica tenha encontrado CPF (indexador) do requerente do certificado digital, com o resultado "positivo", não será necessária a validação de qualquer documento elencado no item "Documentos para efeitos de identificação de um indivíduo" do DOC-ICP-05 [1].

2.5.5 Caso o resultado da verificação biométrica tenha encontrado o CPF (indexador - IDN) do requerente do certificado digital, com o resultado da comparação "negativo", devem comunicar à AC vinculada para que se faça uma análise detalhada do caso. Caso a AR e/ou a AC concluam

que o requerente se trata do titular de fato do documento de identificação e/ou das informações da empresa, deverá ser dado prosseguimento ao processo de emissão do certificado digital. O registro biométrico/biográfico armazenado no banco de dados de forma irregular, tanto da AC quanto do respectivo Sistema Biométrico credenciado devem realizar os procedimentos mencionados no DOC-ICP-05.03 [6] (notificação de irregularidade do registro), comunicando ao ITI sobre a fraude. Caso a AR e/ou a AC concluam que o requerente se trata de um suposto fraudador, não deverá ser emitido o certificado digital e a AC deve comunicar a tentativa de fraude ao ITI.

NOTA 4: Não necessariamente um resultado negativo indica uma tentativa de fraude e/ou que o registro do requerente armazenado no banco de dados biométricos seja de um suposto fraudador. Em alguns casos, por algum processo de deterioração (temporário ou permanente), pode não ser possível verificar a biometria no processo de emissão do certificado digital, sem que o requerente se trate de um suposto fraudador.

NOTA 5: É recomendável que o Sistema Biométrico da ICP-Brasil informe ao AGR qual é o "melhor dedo", no caso de verificação da biometria da impressão digital. Caso nenhuma impressão digital tenha qualidade para verificação, esse requerente não poderá ser identificado pelo processo da verificação biométrica da impressão digital.

NOTA 6: Considerando que o Sistema Biométrico da ICP-Brasil deve ser capaz de verificar, no mínimo, a biometria da impressão digital e da face do requerente, quando não houver possibilidade de utilização da impressão digital, deve-se utilizar outra biometria disponível.

2.5.6 Caso ocorra qualquer indisponibilidade no Sistema Biométrico da ICP-Brasil, deve-se proceder com a verificação obrigatória exigida pela ICP-Brasil e, posteriormente, realizar a consulta pendente quando Sistema Biométrico da ICP-Brasil estiver disponível.

2.5.7 As AC devem manter os arquivos de imagem de todos os dados biométricos coletados de um requerente (que já passaram pelo processo de 1:N no Sistema Biométrico da ICP-Brasil) durante o processo de cadastramento, associados ao dossiê do requerente do certificado digital.

3 COMUNICAÇÃO DE UMA OCORRÊNCIA DE FRAUDE OU INDÍCIO

3.1 O sistema de comunicado de fraude ao ITI passa a ser implementado por meio do preenchimento das informações na interface do sistema de comunicação de fraude da AC, determinado no método descrito no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa). Devem ser preenchidos os seguintes campos na interface do sistema pela AC e, posteriormente, enviados ao ITI:

i. A AC e AR onde ocorreu a fraude ou tentativa (tabela pré-determinada) – obrigatório (lembrando que essas informações não serão replicadas no método de atualização de base da AC, somente serão armazenadas no servidor ITI);

ii. Nome do Informante: quem está cadastrando a fraude – opcional;

iii. CPF do Informante: CPF de quem está cadastrando a fraude – opcional;

iv. UF: escolha da UF onde ocorreu a fraude/indício (tabela pré-determinada) – obrigatório;

v. Município: escolha do município onde ocorreu a fraude/indício (tabela pré-determinada por UF) – obrigatório;

vi. Tipo de Ocorrência: indício ou fraude – obrigatório;

vii. Número do certificado: número de série do certificado se for fraude – obrigatório;

viii. Ocorrência: breve relato do modo de operação do estelionatário, data, tipo de documento apresentado, tipo de certificado fraudado, como foi detectada a fraude/indício (2000 caracteres no máximo) – obrigatório;

ix. Data da ocorrência: data da identificação do indivíduo – obrigatório;

x. Diligência de investigação: como foi detectada a fraude (análise do documento). Caso alguma forma de detecção tenha dado como válido o documento, marcar "válido". Caso a forma de detecção tenha constatado a fraude no documento, marcar como "inválido". Clicar em "Adicionar" para inclusão – opcional;

xi. Nome: nome conforme aparece no documento apresentado – obrigatório;

xii. CPF: número do CPF conforme apresentado no documento – obrigatório;

xiii. Data de nascimento: data conforme apresentado no documento – obrigatório;

xiv. Correio eletrônico: correio eletrônico fornecido do suposto fraudador – opcional;

xv. Telefone: telefone fornecido do suposto cliente – opcional;

xvi. Documento de identidade: caso seja RG/Carteira militar apresentada pelo requerente, fornecer as seguintes informações, caso apareçam no documento: a. número (mesmo apresentando outro tipo de documento que não seja o RG, como, por exemplo, a CNH, escrever o número de identidade que aparece no documento apresentado); b. Data de expedição; c. – obrigatório, se for o caso;

xvii. Certidão: certidões depois de 2009 apresentam uma matrícula (número único), que deve ser colocada no campo "número". Fornecer as informações: a. número (e naturalidade); b. livro; c. folha, caso apareçam no documento (RG, CTPS ou outro) – opcional;

xviii. CNH: caso seja CNH apresentada, fornecer as seguintes informações: a. número; b. data de emissão; c. 1ª habilitação; d. UF expedição; e. data de validade; f. formulário; g. número de identidade – obrigatório, se for o caso;

xix. Passaporte: caso seja Passaporte apresentado, fornecer as seguintes informações: a. número; b. data de expedição; c. data de validade; d. país (tabela pré-determinada) – obrigatório, se for o caso;

xx. CTPS: caso seja CTPS apresentada, fornecer as seguintes informações: a. número; b. data de emissão; c. PIS/PASEP; d. UF (tabela pré-determinada) – obrigatório, se for o caso;

xxi. Outro documento: qualquer outro documento de natureza civil, como, por exemplo, carteira de entidade de classe, que têm por força legal a presunção de identificação, fornecer as seguintes informações: a. número; b. data de emissão; c. nome; d. UF (tabela pré-determinada) – obrigatório, se for o caso;

NOTA 7*:* No campo "outros" do Sistema de Comunicação de Fraude, deve-se, também, realizar o *upload* das imagens em formato WSQ, conforme especificações contidas no DOC-ICP-05.03 [6], das impressões digitais dos supostos fraudadores. Esses arquivos de impressões digitais devem estar nomeados da seguinte forma: 1: Polegar esquerdo; 2: Indicador esquerdo; 3: Dedo médio esquerdo; 4: Anelar esquerdo; 5: Dedo mínimo esquerdo; 6: Polegar direito; 7: Indicador direito; 8: Dedo médio direito; 9: Anelar direito; 10: Dedo mínimo direito. Essas impressões digitais, assim como a face, devem ser submetidas/enviadas pela AC/PSS ao seu respectivo Sistema Biométrico para inserção dessas biometrias no repositório de Lista Negativa biométrica do mesmo.

xxii. Características físicas: devem ser selecionadas as características físicas perceptíveis do suposto fraudador, tais quais: a. cor da pele (seleção: amarelo; branco; indígena; negro; pardo); b. cor dos olhos (seleção: claros; escuros); c. cor predominante do cabelo (seleção: branco; escuro; grisalho; loiro; ruivo); d. deficiências físicas perceptíveis (seleção: cadeirante; cego; manco; mudo; surdo); e. idade aparente (seleção: A – menor que 30 anos; B – entre 30 e 50 anos; C – mais de 50 anos); f. sexo (seleção: masculino; feminino); g. sinais corporais perceptíveis (seleção: falta de dedos nas mãos; mancha na pele; marcas como cicatrizes; tatuagem ou sinais em membros superiores; tatuagem ou sinais no rosto ou pescoço); h. tipo de cabelo (seleção: calvo; curto; longo; médio) – opcional;

NOTA 8: Deve se ter certeza da informação antes de adicionar as características físicas do fraudador. Em caso de dúvida, deve-se deixar uma ou mais informações físicas sem serem adicionadas. Como essas informações serão utilizadas posteriormente por todas as ACs para as pesquisas por características físicas na Lista Negativa da AC, é fundamental que estejam corretas para que se tornem eficientes.

xxiii. Informações da empresa: fornecer as seguintes informações: a. CNPJ; b. razão social; c. endereço; d. telefone; e. CEP; f. CNAE; g. UF (tabela pré-determinada); h. Município (tabela pré-determinada por UF) – obrigatório, se for o caso;

xxiv. *Upload* da imagem do documento de identificação e da face: deve ser enviado a imagem do documento de identificação (escolher tipos: RG, CNH, CTPS, PASSAPORTE, OUTROS) e da face (escolher o tipo FOTO) disposta em pé do suposto fraudador no comunicado – obrigatório;

NOTA 9: Imagem do documento de identificação em formato (JPG ou JPEG), com a face do

requerente disposta em pé, nomeado com o CPF do mesmo (exemplo: 11122233344.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB, em que se possa ler nitidamente todas as informações biográficas apresentadas no documento. Imagem da face em formato (JPG ou JPEG), com a face do requerente disposta em pé, nomeado com o CPF"FACE" do mesmo (exemplo: 11122233344FACE.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB (pode ser recortada do próprio documento de identificação).

xxv. Após todo o preenchimento dos campos do comunicado e *upload* das imagens, deve-se fazer uma verificação de todas as informações inseridas. Caso estejam corretas, deve ser enviado o comunicado ao ITI, conforme descrito no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa).

NOTA 10: Qualquer cancelamento de fraude, feito pelas AC por processos de auditoria e análise detalhada devem ser enviadas ao endereço de correio eletrônico: comunicafraude@iti.gov.br, com a descrição detalhada dos motivos do cancelamento.

3.2 A AC emissora do certificado digital deve notificar, ou cuidar para que se notifique, a autoridade policial competente mais próxima do ocorrido, a fraude em sua emissão.

3.3 Após o registro na lista negativa, encaminhar à DAFN o dossiê de emissão do certificado, os dossiês dos AGR que atuaram na identificação e cópia do Boletim de Ocorrência.

4 DOCUMENTOS REFERENCIADOS

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

Ref.	*Nome do documento*	*Código*
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[3]	CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[4]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

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

Ref.	*Nome do documento*	*Código*
[5]	MÉTODOS WEBSERVICE LISTA NEGATIVA E COMUNICADO DE FRAUDE	ADE-ICP-05.02.B
[6]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03
[7]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01