INSTRUÇÃO NORMATIVA ITI N° 10, DE 22 DE OUTUBRO DE 2020

Aprova a versão revisada e consolidada do documento Características Mínimas de Segurança para as AR da ICP-Brasil – DOC-ICP-03.01.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9° do anexo I do Decreto n° 8.985, de 8 de fevereiro de 2017, pelo art. 1° da Resolução n° 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2° da Resolução n° 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020,

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

CONSIDERANDO que a Lei n° 14.063, de 23 de setembro de 2020, restabeleceu o amparo legal para a emissão primária de certificados digitais ICP-Brasil de forma não presencial e que a Resolução CG-ICP Brasil n° 177, de 20 de outubro de 2020, delegou à AC Raiz a regulamentação dos procedimentos e requisitos técnicos a serem utilizados na identificação por videoconferência,

RESOLVE:

Art. 1° Esta Instrução Normativa aprova a versão revisada e consolidada do documento Características Mínimas de Segurança para as AR da ICP-Brasil - DOC-ICP-03.01.

Art. 2° Fica aprovada a versão 4.0 do documento DOC-ICP-03.01 – Características Mínimas de Segurança para as AR da ICP-Brasil.

Art. 3° Ficam revogadas:

I - a Instrução Normativa n° 02, de 31 de julho de 2008;

II - a Instrução Normativa n° 09, de 17 de novembro de 2010;

III - a Instrução Normativa n° 05, de 25 de maio de 2012;

IV - a Instrução Normativa n° 05, de 06 de abril de 2018; e

V - a Instrução Normativa n° 11, de 19 de setembro de 2018.

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

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

ANEXO

CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL

DOC-ICP-03.01

Versão 4.0

22 de outubro de 2020

SUMÁRIO

Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Instrução Normativa ITI nº10, de 22.10.2020 Versão 4.0	Nova versão integral	Revisão e consolidação do DOC-ICP-03.01, conforme Decreto nº 10.139, de 28 de novembro de 2019. Adequação para emissão por meio de videoconferência.
Resolução nº 154, de 01.10.2019 Versão 3.1	4.1.2, alínea "m"	Alínea revogada.
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".

Ato que aprovou a alteração	Item alterado	Descrição da alteração
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 18.11.2010 Versão 1.4	2.2.4, 4.2.1, 6.1.7	Alteração dos itens citados para adequação ao 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
CG	Comitê Gestor
FCT	Fonte Confiável do Tempo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
OM-BR	Objetos Metrológicos ICP-Brasil
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócios
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 ARs 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 e o encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e a identificação de seus solicitantes, na forma e condição regulamentada no DOC-ICP-05 [1].

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 do requerente de certificado** – Compreende a etapa de confirmação da identidade de um indivíduo ou de uma organização, na forma e condição regulamentada no DOC-ICP-05 [1], para posterior emissão do certificado.

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.

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 (sete) anos.

5 SEGURANÇA DE REDE

A AR deve encaminhar as solicitações de emissão ou de revogação de certificados à AC utilizando VPN, SSL ou outra tecnologia de igual ou superior nível de segurança e privacidade.

6 SEGURANÇA DA INFORMAÇÃO

6.1 Diretrizes Gerais

6.1.1 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.

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

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

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

6.1.5 O Inventário de Ativos deve relacionar, pelo menos:

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

b) softwares instalados nos equipamentos, atualizado mensalmente.

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

6.1.5.2 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

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 [1].

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** Aprovado pela Resolução nº 08, de 12 de dezembro de 2001	**DOC-ICP-05**
[2]	**POLÍTICA DE SEGURANÇA DA ICP-BRASIL** Aprovado pela Resolução nº 02, de 25 de setembro de 2001	**DOC-ICP-02**
[3]	**CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL** Aprovado pela Resolução nº 06, de 22 de novembro de 2001	**DOC-ICP-03**
[5]	**CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL** Aprovado pela Resolução nº 24, de 29 de agosto de 2003	**DOC-ICP-08**
[6]	**CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL** Aprovado pela Resolução nº 25, de 24 de outubro de 2003	**DOC-ICP-09**

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[7]	**PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL** Aprovado pela Instrução Normativa nº 4, de 18.05.2006	**DOC-ICP-01.01**

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[4]	FORMULÁRIO DE CREDENCIAMENTO DE AR	ADE-ICP-03.B

9.4 Referências bibliográficas

RFC 8017, IETF - PKCS #1: RSA Cryptography Specifications version 2.2, november 2016