Infraestrutura de Chaves Públicas Brasileira

CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL

DOC-ICP-03.01 - Versão 2.2

19 de setembro de 2017

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
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	1.6 e 4.1.2.”k”	Incluída a referência [3] ao item 1.6 e indicação 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 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	-	Aprovar a versão 1.0 do documento

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
19.05.2006 Versão 1.0		

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
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
ITS	Instalação Técnica Secundária
NBR	Norma Brasileira
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. Estes regulamentos aplicam-se a todas as AR integrantes da ICP-Brasil e devem ser observados em todas suas instalações técnicas e postos provisórios. Quando houver procedimentos que devam ser observados, especificamente, por apenas um tipo de instalação, esse fato será assinalado.

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 validação e verificação da solicitação de certificados.

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, validação, verificação 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 individuo** - 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, instalação técnica ou posto provisório 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 da instalação técnica** – Conjunto de documentos relativos à instalação técnica: Plano de Continuidade de Negócios, Análise de Risco e outros citados no item 6.1.2 deste documento.

h) **Dossiê do titular de certificado** – Conjunto formado pela cópia dos documentos de identificação utilizados para emissão do certificado e pelos termos de titularidade, e pela solicitação de revogação, quando for o caso.

i) **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.

j) **Instalação técnica** - Ambiente físico de uma AR, cujo funcionamento foi devidamente autorizado pelo ITl, onde são realizadas as atividades de validação e verificação da solicitação de certificados. Não possui período de tempo determinado para funcionamento.

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

l) **Ponto de Centralização da AR** – Local, no exterior ou em território nacional, onde a AR armazena os dossiês de todos os seus Agentes de Registro e pode armazenar também os dossiês de titulares de certificados da ICP-Brasil.

m) **Posto provisório** – Ambiente montado pela AR, fora de suas instalações técnicas, para realização das atividades inerentes às autoridades de registro. Possui período de tempo determinado para funcionamento.

n) **Responsável pela instalação técnica ou posto provisório** – Pessoa indicada para tal, conforme informado quando da solicitação de credenciamento da AR ou da solicitação de autorização de funcionamento da instalação técnica ou posto provisório.

o) **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.

p) **Validação da solicitação de certificado** – Compreende as etapas 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 a etapa de emissão do certificado.

q) **Verificação da solicitação de certificado** - Confirmação da validação de uma solicitação de certificado.

r) **Instalação Técnica Secundária** - Ambiente físico de uma AR, cujo funcionamento foi devidamente autorizado pelo ITI, onde é realizada exclusivamente a atividade de coleta e/ou verificação biométrica e validação da solicitação de certificados. Não possui período de tempo determinado para funcionamento;

s) **Validação Externa** – compreende a realização da etapa de validação da solicitação de certificado e coleta biométrica do titular do certificado fora do ambiente físico da AR, nas hipóteses e na forma prevista no item 3.1.1.2 do DOC-ICP-05 [1].

1.4. Os critérios e procedimentos para credenciamento de uma AR, de novas instalações técnicas de AR já credenciada e para abertura de posto provisório de 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, utilizando-se de instalações técnicas e/ou postos provisórios igualmente autorizados.

1.6. Em caso de alteração de endereço da instalação técnica ou da instalação técnica secundária, o fato deve ser previamente reportado à AC responsável, que enviará ao ITI formulário de credenciamento ADE-ICP-03.E [4] com dados atualizados, solicitando nova autorização de funcionamento, acompanhado dos documentos previstos no DOC-ICP-03 [3].

1.7. É vedada a alteração de endereço de posto provisório de AR após a autorização de funcionamento dada pelo ITI, mediante intimação da solicitante.

1.8. 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].

2. SEGURANÇA DE PESSOAL

2.1. Disposições Gerais

2.1.1. Os normativos que tratam da segurança de pessoas estão no item 7 do DOC-ICP-02 [2] e no item 5.3 do 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.

2.1.3. Pode ser firmado acordo documentado, entre AC e AR, no qual a AC delega à AR a atividade de incluir/excluir Agentes de Registro no aplicativo de AR, desde que a AR não possua agente de registro como sócio. Nesse caso, o responsável por essa atividade, na AR, deve ser formalmente designado e possuir âmbito de atuação restrito ao necessário às atividades daquela AR.

2.1.4. 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 por instalação técnica, 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 item 7.3.8 do DOC-ICP-02 [2];

j) cópia do documento, gerado em meio digital ou em papel, que comprove que a AR executou (nos casos previstos no item 2.1.3) ou solicitou à AC a habilitação do Agente de Registro no sistema de certificação;

k) confirmação da AC ou AR (nos casos previstos no item 2.1.3) 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) cópia do documento, gerado em meio digital ou em papel, que comprove que a AR executou (nos casos previstos no item 2.1.3) ou solicitou à AC a desabilitação do Agente de Registro no sistema de certificação;

b) confirmação da AC ou AR (nos casos previstos no item 2.1.3) quanto à desabilitação do Agente de Registro no sistema de certificação;

c) declaração assinada pelo Agente de Registro de que não possui pendências, conforme previsto no item 7.3.2 do DOC-ICP-02 [2];

d) 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 externo independente, cadastrado junto à ICP-Brasil conforme DOC-ICP-08 [5];

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

d) 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 ou AR (nos casos previstos no item 2.1.3) 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.

NOTA: Para a emissão de certificado que integra o Documento RIC, é admitida a inclusão nas bases de dados, bem como a concessão de permissões de acesso ao sistema de certificação, de funcionário de Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC.

2.2.5. Os dossiês de todos os Agentes de Registro da AR devem ficar em um mesmo ponto de centralização da AR, 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 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 bi-anualmente, 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 ou efetuada pela AR, conforme o caso.

2.4.4. A AR 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 são documentados e esses documentos são arquivos no dossiê do Agente, em poder da AR.

2.5.2. A AR executa (nos casos previstos no item 2.1.3) ou solicita à AC a revogação das permissões de acesso ao sistema de certificação, informando o motivo da suspensão ou desligamento do Agente de Registro. O responsável designado para essa tarefa expede a ordem de revogação da permissão de acesso ao sistema. Esses processos são documentados e esses documentos são arquivados na cópia do dossiê do Agente de Registro.

3. SEGURANÇA FÍSICA

3.1. As instalações técnicas e os postos provisórios de uma AR podem ser de 2 tipos:

a) ambiente dedicado às atividades da AR;

b) ambiente compartilhado com outras atividades da organização.

3.2. Para ambos os casos, aplicam-se as seguintes exigências mínimas de segurança:

a) equipamentos de prevenção de incêndios;

b) armário ou gabinete com chave, de uso exclusivo da AR, para a guarda de documentos da AR;

c) os circuitos elétricos de alimentação dos equipamentos de processamento de dados deverão ser protegidos por *no-break* ou estabilização de tensão.

d) os circuitos elétricos e lógicos deverão ser protegidos por tubulação e/ou canaletas adequadas.

3.3. Para as AR que possuem ambiente dedicado, aplicam-se, além das exigências do item 3.2, também as seguintes:

a) controle de acesso ao ambiente, com autorização de acesso apenas para os agentes de registro e titulares de certificados;

b) porta única de entrada, com fechadura tetra;

c) paredes que previnam o acesso não autorizado, inclusive pela parte superior, constituídas de alvenaria de tijolos, painéis de gesso acartonado, divisórias removíveis ou de material de resistência equivalente;

d) iluminação de emergência.

OBS.: caso a sala possua janelas ou qualquer outra abertura para o ambiente externo do prédio, essas devem ser lacradas ou gradeadas, para impedir o acesso externo.

3.4. Para as AR que possuem ambiente compartilhado aplicam-se, além das exigências do item 3.2, também as seguintes:

a) vigilância ostensiva ou monitoramento por CFTV no ambiente da AR;

b) controle de acesso ao prédio ou ao ambiente onde está instalada a AR.

3.5. O monitoramento por CFTV pode ser realizado pela própria AR ou por empresa de segurança contratada. A câmara deve filmar o ambiente e equipamentos da AR e as imagens devem ser mantidas por 60 dias, em ambiente seguro.

3.6. Para os casos específicos de postos provisórios instalados em feiras e eventos com período de funcionamento máximo de 15 dias ficam dispensadas essas exigências de segurança do item 3.4. Fica também dispensada a exigência 3.2.b, desde que os documentos e equipamentos sejam levados para armazenamento em uma instalação técnica da AR, no encerramento diário das atividades do posto provisório.

3.7. As atividades da AR relativas a validação da solicitação de certificados podem ser executadas externamente ao ambiente da AR, desde que observado o disposto no item 3.1.1.1 e 3.1.1.2. do DOC-ICP-05 [1].

3.8. As ARs somente poderão utilizar a modalidade de validação externa depois de adaptar seus computadores móveis ao disposto no item 4.1.2, e desde que a AC à qual a AR se vincula tenha adaptado seus procedimentos, seu sistema de certificação e o aplicativo da AR a todas as regras deste documento e ao disposto no item 3.1.1.2 do DOC-ICP-05 [1].

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.

4.1.2. 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) exigência de uso de senhas fortes;

c) diretivas de senha e de bloqueio de conta;

d) *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 sistema dos operadores da AR;

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.

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

f) *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;

g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;

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

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

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

k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

l) para equipamentos utilizados em Postos Provisórios, Instalações Técnicas Secundárias e em procedimento de validação externa, utilização de aplicativo de georreferenciamento que permite rastrear o computador, sendo que a localização do equipamento deve ficar disponível no sistema de AR;

m) equipamentos de coleta biométrica, em atendimento aos padrões da ICP-Brasil, para garantir mecanismo de coleta biométrica no qual seus registros sejam processados e enviados ao sistema sem permitir a manipulação pelo agente de registro;

n) equipamentos que exijam a identificação biométrica do agente de registro durante a identificação biométrica do requerente do certificado e que exija a identificação biométrica do responsável pela execução de todas as etapas do processo de validação e verificação do certificado digital.

4.1.3. Os *logs* de auditoria do sistema operacional devem registrar os acessos aos equipamentos e devem ficar armazenados localmente por um período mínimo de 60 dias.

4.1.4. A análise desses *logs* somente precisa 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. É desejável que o Agente de Registro não possua perfil de administrador ou senha de *root* dos equipamentos, ficando essa tarefa delegada a terceiros da própria organização, para permitir segregação de funções.

4.1.6. As estações de trabalho da AR, incluindo equipamentos portáteis utilizados na instalação técnica secundária para executar os procedimentos de validação, podem ser utilizados para atendimento de validação externa, não podendo ser utilizados em outras atividades fora do endereço autorizado pelo ITI, desde que atendidos os demais requisitos constantes nas normas da

ICP-Brasil.

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 ou, para tratar de certificado que integra Documento RIC, de funcionário de Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009, 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 4.5.1 do DOC-ICP-05 [1];

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

f) registro em *log*, para em cada certificado emitido, informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR;

g) mecanismo para revogação automática dos certificados digitais emitidos fora do ambiente da AR e que não tenham sido verificados pelo segundo Agente de Registro, mediante cópia da documentação apresentada na etapa de validação, até o momento do início da validade do certificado.

h) registrar as coordenadas de georreferenciamento associada à data e hora do momento da autenticação biométrica do agente de registro e do momento da coleta biométrica do titular do certificado, para cada certificado a ser emitido.

NOTA: A tecnologia de georreferenciamento utilizada pelo aplicativo de AR deve garantir a posição do local onde as atividades de validação do certificado digital ocorrem, vedando a utilização de tecnologia cuja localização é obtida através de endereçamento IP (*Internet Protocol*) incluindo sistema de VPN (*Virtual Private Network*) ou tecnologias similares.

4.2.2. Para atendimento do previsto no item 6.1 do DOC-ICP-05, 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.

OBS.: Exclusivamente para as versões de aplicativos de AR que já se encontrem em produção, na data de publicação da presente instrução, ficam dispensados os itens c, d, e.

4.2.3. Os *logs* gerados por esse aplicativo devem ser armazenados na AC pelo prazo de 6 anos, conforme previsto no item 4.6.2. do DOC-ICP-05.

5. SEGURANÇA DE REDE

5.1. Cada instalação técnica ou posto provisório da AR que tenha prazo de duração maior do que 15 dias deverá elaborar diagrama da topologia de rede de comunicação entre a AR e a AC, que deve ser mantido sempre atualizado. Esse documento deve estar arquivado no dossiê instalação técnica ou posto provisório.

5.2. 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

6.1.1. Todas as informações e documentos da instalação técnica ou posto provisório da AR devem ser classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme DOC-ICP-02 [2].

6.1.2. Cada instalação técnica ou posto provisório de AR deve possuir um dossiê, contendo cópia dos seguintes documentos, atualizados:

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], capítulos 12 e 13.

6.1.4. Para os casos específicos de postos provisórios instalados em feiras e eventos com período de funcionamento máximo de 15 dias fica dispensada a elaboração de Análise de Risco e Plano de Continuidade de Negócios.

6.1.5. Uma cópia do PCN deverá ser armazenada em local seguro, fora da sala da AR.

6.1.6. O Inventário de Ativos deve estar sempre atualizado, mantendo histórico das alterações e deve ser assinado pelo responsável pela instalação técnica ou posto provisório.

6.1.7. O Inventário de Ativos deve relacionar, pelo menos:

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

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

c) equipamento de Órgãos de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009, utilizados para acessar o sistema da AC.

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

6.1.7.2. 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 da instalação técnica, da instalação técnica secundária e do posto provisório devem ser guardados, obrigatoriamente, no armário chaveado quando se tratar de documentos físicos ou em ambiente computacional protegido com senha, da AC ou da AR, quando se tratar de documentos eletrônicos, em todos os casos, com acesso permitido somente aos agentes de registro.

6.2.2. A AR 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, mas os originais não podem ser destruídos, devendo permanecer arquivados no ponto de centralização da AR 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 ou responsáveis designados formalmente para trabalhar com os documentos;

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

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

a) em um dos pontos de centralização da AR, para aquelas que possuam mais de uma instalação técnica; ou

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

c) na AC emissora para os casos de certificados A CF-e-SAT (dossiê eletrônico).

6.2.4. A critério de cada AR, pode ser mantida cópia do dossiê na instalação técnica ou posto provisório onde foi gerado, o que não substitui o armazenamento do original num dos locais citados acima.

6.2.5. 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), no prazo máximo de 30 dias corridos, a partir da geração do dossiê.

6.2.6. A AR 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.

6.2.7. Para AR instaladas em território nacional, o ponto de centralização deve ser, também, em território nacional. Cada estado da federação deve possuir no máximo um ponto de centralização para dossiês de agentes de registro e um ponto de centralização para dossiês de titulares de certificados, podendo tais pontos estarem no mesmo local. Para estados da federação com população maior que 10 milhões de habitantes, a AR poderá criar até 3 pontos de centralização para dossiês de agentes de registro e até 3 pontos de centralização para dossiês de titulares de certificados, se desejado. Um mesmo ponto pode centralizar documentos de diferentes estados ou regiões. A localização desse(s) ponto(s) e sua área de abrangência devem ser informadas ao ITI, bem como qualquer alteração que venha a ser feita posteriormente.

6.2.8. Para AR instaladas no exterior, o ponto de centralização deve ser único, no próprio país onde estão localizadas ou no Brasil.

6.2.9. O Ponto de Centralização da AC e o ponto de centralização da AR devem possuir requisitos de segurança física e/ou lógica no mínimo equivalentes ao de uma instalação técnica de AR e sua localização deve ser informada ao ITI, bem como qualquer alteração que venha a ser feita posteriormente.

6.2.10. 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 cópias não utilizadas de documentos dos titulares de certificados, termos de titularidade descartados, diagramas de rede etc.

6.2.11. 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.

6.2.12. O dossiê do titular do certificado A CF-e-SAT 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.

7. CICLO DE VIDA DO CERTIFICADO

7.1. Os processos que dizem respeito ao ciclo de vida do certificado - solicitação, validação e verificação da solicitação, emissão e revogação - estão descritos nos itens 3 e 4 do documento DOC-ICP-05.

7.2. As AC devem implementar qualquer forma sistematizada de consulta/validação de um ou mais dos dados biográficos constantes da Cédula de Identidade (CI) apresentada pelo requerente do certificado digital para efeito de identificação de indivíduo, com base nas normas e regras dos órgãos emissores do documento de identidade, sem prejuízo às outras consultas obrigatórias.

7.3. Caso seja apresentada a Carteira Nacional de Habilitação – CNH, a AR deverá proceder a verificação por meio de consulta à base de dados dos órgãos emissores da CNH. Caso a AR perceba que a CNH possui dados não convergentes aos pesquisados, a AR deverá validar essa informação com uma outra fonte de consulta.

8. ACORDOS OPERACIONAIS

8.1. Conforme previsto no item 3.2.5 do DOC-ICP-03 [3], é permitido às AR credenciadas na ICP-Brasil celebrar entre si Acordos Operacionais para que uma execute, em nome da outra, as atividades de validação e verificação da solicitação de certificado.

8.2. Esses Acordos devem possuir pelo menos as seguintes cláusulas:

a) identificação das AR celebrantes do acordo, com a data de publicação, no DOU, de seu credenciamento na ICP-Brasil e os números de processos respectivos;

b) identificação das atribuições que caberão a cada uma das AR, em função do acordo;

c) identificação do local e responsável pela guarda dos dossiês de titulares de certificados, inclusive no caso de encerramento do acordo;

d) compromisso de que as AR celebrantes do acordo respeitem as normas da ICP-Brasil, em todos os procedimentos executados;

e) prazo pelo qual o acordo é celebrado;

f) obrigação da AR contratante de verificar a conformidade dos processos executados pela AR contratada.

8A. DAS VEDAÇÕES

8A.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.

8A.2. É vedada qualquer outra forma de emissão de certificado, fora das hipóteses previstas na legislação e nas normas que regem a ICP-Brasil, qualquer que seja a denominação utilizada, aí incluídas, mas não limitadas às figuras denominadas ponto de atendimento, posto de validação,

parceiro, canal, agente credenciado, franquia, agência autorizada ou por qualquer outra forma não expressamente prevista na legislação.

8A.3. É vedado delegar ou transferir a terceiros, não credenciados, atividades privativas das entidades credenciadas ou autorizadas pelo ITI, a qualquer título.

8A.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, inclusive quando emitidos em instalações técnicas ou por procedimento de validação externa, que não tenham atendido os requisitos estabelecidos na regulamentação, ressalvado o direito de terceiros de boa-fé.

8A.5. É proibido a divulgação por parte das AC e AR, em qualquer veículo de comunicação, suporte ou sítios de internet, endereços de locais de atendimento ao usuário que não estejam credenciados ou autorizados pelo ITI.

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
[4]	Formulário SOLICITAÇÃO DE FUNCIONAMENTO DE NOVOS ENDEREÇOS DE INSTALAÇÕES TÉCNICAS DE AR	**ADE-ICP-03.E**