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 1.7

03 de julho de 2018

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
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 (DOC-ICP-05.02).

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 validação e verificação da identidade do requerente e das comunicações de 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 validação e verificação 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, 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 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) Instalação técnica – Ambiente físico de uma AR, cujo funcionamento foi devidamente autorizado pelo ITI, onde são realizadas as atividades de validação e verificação da solicitação de certificados. Não possui período de tempo determinado para funcionamento.

g) 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/ou identificação biométrica, e a etapa de emissão do certificado.

h) Verificação da solicitação de certificado – Confirmação da validação de uma solicitação de certificado.

i) 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 eletrônicos de titulares de certificados da ICP-Brasil e deve armazenar eletronicamente os documentos de identificação, fotografia da face e impressões digitais do requerente.

j) Central de Verificação – Modelo que pode ser adotado pelas AC na qual realizam todo o processo de verificação da documentação do requerente em instalação técnica de AC.

l) 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.

m) Sistema Biométrico ICP-Brasil – Uma ou mais entidades Prestadoras de Serviço Biométrico - PSBio, credenciadas 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. IDENTIFICAÇÃO E AUTENTICAÇÃO

2.1. Registro Inicial

2.1.1. Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados no DOC-ICP-05:

a) 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 e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim;

b) 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;

NOTA 1: A procuração do representante legal deve ser específica para fins de emissão de um certificado digital ICP-Brasil e o ato constitutivo da pessoa jurídica deve explicitar essa

possibilidade de representação por procuração.

c) 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.

2.1.2. Verificação da solicitação de certificado – confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

a) por AGR distinto do que executou a etapa de validação;

NOTA 2: Preferencialmente os AGR devem ser segregados fisicamente.

b) em uma das instalações técnicas da AR ou instalação técnica de AC devidamente autorizadas a funcionar pela AC Raiz;
c) somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;
d) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

2.1.3. O processo de validação poderá ser realizado pelo AGR fora do ambiente físico da AR, desde que utilizado ambiente computacional auditável e devidamente registrado no inventário de *hardware* e *softwares* da AR.

2.1.4. Todas as etapas dos processos de validação e verificação da solicitação de certificado deverão ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. Tais registros deverão ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

2.2. Autenticação da identidade do requerente

Conforme estabelecido no DOC-ICP-05, 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.

2.2.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a documentação a seguir, em sua versão original, e coletada as seguintes biometrias para fins de identificação de um indivíduo solicitante de certificado.

a) Cédula de Identidade ou Passaporte, se brasileiro;

b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;

c) Passaporte, se estrangeiro não domiciliado no Brasil;

d) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial;

e) Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4;

f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [10];

g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [10].

2.2.1.1 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.

NOTA 3: Entende-se como Cédula de Identidade os documentos 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.

NOTA 4: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento.

2.2.2. Os AGR deverão realizar uma análise detalhada do documento de identificação, principalmente do RG e CNH, conforme o disposto no ADE-ICP-05.02.A (Procedimentos de Verificações e Validações dos Documentos de Identificação).

2.2.3. As AC deverão implementar qualquer forma sistematizada (consultas a bases oficiais, auxílio de *softwares* e/ou peritos) de consulta/validação de um ou mais dos dados biográficos, constantes da Cédula de Identidade, apresentados pelo requerente do certificado digital para efeito de validação e/ou verificação do documento de identificação do requerente, com base nas normas e regras dos órgãos emissores do documento de identidade.

NOTA 6: A AR deve proceder a verificação por meio de consulta à base de dados dos órgãos emissores da Carteira Nacional de Habilitação – CNH quando for utilizada a CNH como documento de identificação, mesmo que sua data de validade esteja expirada, hipótese em que

haverá restrição de informações para validação.

2.2.3.1. Os resultados, sem irregularidades, dessa consulta/validação deverão ser apensados ao dossiê do titular do certificado.

2.2.3.2. Caso os resultados das consultas/validação tenham dado como resposta "documento válido", os AGR devem, mesmo assim, realizar as validações e verificações elencadas nos subitens 2.2.1 e 2.2.2. Caso a AR conclua pela validade do documento de identificação, deve prosseguir com o processo de emissão do certificado digital. Caso a AR conclua pela não validade do documento, deve comunicar a AC para que essa faça o comunicado de tentativa de fraude ao ITI, conforme disposto do item 3.

2.2.3.3 Caso os resultados das consultas/validação tenham dado como resposta "documento inválido", os AGR, além de realizarem as validações e verificações elencadas nos subitens 2.2.1 e 2.2.2, devem comunicar a AC vinculada para que se faça uma análise detalhada do caso. Caso a AR e/ou AC concluam pela não emissão do certificado digital, a AC deve fazer o comunicado de tentativa de fraude ao ITI, conforme disposto do item 3. Caso a AR e/ou AC concluam pela validade do documento de identificação, deve prosseguir com o processo de emissão do certificado digital.

2.2.4. As AC devem disponibilizar, para as AR vinculadas à sua respectiva cadeia, uma interface para consulta a base de dados da Lista Negativa da AC, por meio do próprio sistema de emissão de certificados, com os mesmos requisitos de segurança e disponibilidade, em cada processo de emissão de um certificado digital ICP-Brasil.

2.2.4.1. 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 (Métodos de Interface do Serviço de Lista Negativa).

2.2.4.2. A interface da aplicação deve disponibilizar para os AGR, no mínimo, as seguintes consultas/pesquisas ao banco de dados da Lista Negativa da AC:

i. Consulta aos dez maiores supostos fraudadores da ICP-Brasil. Os AGR devem consultar, na tela da aplicação, as faces dos dez maiores supostos fraudadores da ICP-Brasil.

ii. Consulta aos comunicados de indícios ou fraudes dos últimos sete dias. Os AGR devem consultar, na tela da aplicação, as últimas ocorrências de fraudes relatadas.

- UF em que ocorreu o indício ou fraude (tabela IBGE);
- cidade em que ocorreu o indício ou fraude (tabela IBGE);
- indício ou fraude;
- relato da ocorrência;
- data da ocorrência;
- diligência da investigação (modo como foi detectada o indício ou fraude);
- dados biográficos do indivíduo (todos os dados apresentados no documento de identificação da pessoa física);
- características físicas, 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 (vitiligo por exemplo); 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);

- informações da empresa (apresentados no contrato social ou na Receita Federal), se for o caso;
- face do documento apreendido ou imagem da face de quem pratica a ocorrência;
- imagem de todo documento de identificação da ocorrência;

iii. Pesquisas pelas características físicas do requerente. Os AGR devem pesquisar, na interface da aplicação, pelas características físicas notoriamente visíveis do requerente, elencadas na alínea "ii", deste subitem. Com o resultado das pesquisas se deve verificar, e constatar, se a face apresentada na interface da aplicação não é a do requerente do certificado digital. Caso a pesquisa apresente muitos resultados, e não há certeza sobre a inclusão de outras características físicas, os AGR devem relacionar essa pesquisa a outros campos como, por exemplo, UF ou Município em que a AR está localizada, para reduzir o número de faces apresentadas nesta consulta. A interface deve possibilitar aos AGR uma pesquisa/resultado por todos os campos selecionados, ou seja, mais específica, e por qualquer campo selecionado, ou seja, mais ampla;

iv. Pesquisas pelas informações biográficas das ocorrências. Os AGR, caso não tenha encontrado a face do requerente nas consultas/pesquisas elencadas nas alíneas "i", "ii" e "iii", devem pesquisar na interface da aplicação, no mínimo, pelas seguintes informações apresentadas nos documentos e/ou fornecidas pelo requerente: nome; CPF; correio eletrônico (se houver); razão social (se houver); CNPJ (se houver), usando sempre a forma de busca por qualquer campo selecionado, ou seja, mais ampla. Caso não se obtenha qualquer resultado, deve ser realizada uma busca por fraudadores na região em que a AR está operando – UF e Município. Essa região pode, também, estender-se por UFs próximas (por exemplo: SP e RJ) ou mais específicas como o Municípios próximos. Caso essa pesquisa (UF e Município) apresente um resultado muito extenso, é recomendável que se adicione outros campos de características físicas do requerente, conforme relatado na alínea "iii", deste subitem.

2.2.4.3. Os resultados, sem irregularidades, das consultas/pesquisas a Lista Negativa deverão ser apensados ao dossiê do titular do certificado.

NOTA 7: Todos os registros das pesquisas dos AGR na Lista Negativa devem ser guardados pelo período mínimo de 6 anos pelas AC, conforme o disposto no DOC ICP 05.

2.2.4.4. Caso os resultados das consultas/pesquisas concluam pela ausência do requerente do certificado digital na Lista Negativa, os AGR devem prosseguir com as validações e verificações

elencadas nos subitens 2.2.1, 2.2.2 e 2.2.3.

2.2.4.5. Caso os resultados das consultas/pesquisas constatem que o requerente do certificado digital integra a Lista Negativa, com a imagem da face e/ou do documento de identificação coincidente com o apresentado pelo requerente, os AGR devem realizar as validações e verificações elencadas nos subitens 2.2.1, 2.2.2 e 2.2.3 e, preferencialmente, comunicar à AC vinculada para que se faça uma análise detalhada do caso. Caso a AR e/ou a AC concluam pela não emissão do certificado digital, a AC 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.

2.2.4.6. Caso os resultados das pesquisas a Lista Negativa tenham encontrado as informações biográficas do requerente e/ou da empresa, com a imagem da face e/ou do documento de identificação não coincidente com o apresentado pelo requerente, os AGR, além de realizarem as validações e verificações elencadas nos subitens 2.2.1, 2.2.2 e 2.2.3, devem comunicar à AC vinculada para que se faça uma análise detalhada do caso. Caso a AR e a AC concluam que o requerente se trata do titular de fato do documento de identificação e/ou das informações da empresa, deve prosseguir com o processo de emissão do certificado digital. Caso a AR e a AC concluam que se trata de outro suposto fraudador, utilizando as informações biográficas da pessoa e/ou da empresa já cadastradas no banco de dados da Lista Negativa, não se deve emitir o certificado digital e a AC deve comunicar a tentativa de fraude ao ITI, conforme disposto do item 3.

2.2.4.7. Caso ocorra qualquer indisponibilidade no banco de dados da Lista Negativa da AC, não deve ser emitido o certificado digital.

2.2.4.8. As informações contidas nas consultas/pesquisas feitas à Lista Negativa advêm dos documentos de identificação e das empresas que por algum motivo incorreram em alguma irregularidade no processo de emissão, culminando no registro de ocorrências pelas AC (ou pelo ITI no processo de auditoria/fiscalização). Entretanto, é possível o registro na Lista Negativa de ocorrência de fraudes ou tentativas por meio da utilização de informações verdadeiras de pessoa e/ou empresa, sem o conhecimento do titular da documentação. Por essa razão, observado qualquer indício de irregularidade, serão necessárias as devidas averiguações, conforme disposto neste subitem 2.2.4, e as devidas comunicações (de tentativa ou de cancelamento de fraude), conforme disposto no item 3.

2.2.5. As AC devem disponibilizar, para todas as AR vinculadas à 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.

2.2.5.1. O Prestador de Serviço Biométrico 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, DOC-ICP-03, DOC-ICP-08 e DOC-ICP-09.

2.2.5.2. 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.

2.2.5.3. 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.

NOTA 8: Todos os logs de transação biométrica feitos pelo AGR devem ser guardados pelo período de 6 anos pelas AC, conforme disposto no DOC-ICP-05.

2.2.5.4. Caso o resultado da verificação biométrica não tenha encontrado o CPF (indexador) do requerente do certificado digital, os AGR devem prosseguir com as outras validações e verificações elencadas no DOC-ICP-05.02.

NOTA 9: Em caso de validação e verificação sem irregularidades dos documentos, as informações biométricas/biográficas do requerente devem ser armazenadas pelas AC e enviadas ao Sistema Biométrico da ICP-Brasil credenciado pelo ITI. O registro do requerente cadastrado deve ser único para toda ICP-Brasil, portanto, se houver mais de uma entidade credenciada, elas devem garantir a unicidade dos cadastramentos.

NOTA 10*:* 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.

2.2.5.5. Caso o resultado da verificação biométrica tenha encontrado CPF (indexador) do requerente do certificado digital, com o resultado "positivo", a AR deverá convalidar o CPF com outras informações biográficas do requerente, por meio de consulta às entidades oficiais ou pelos processos de validação e verificação descritos em norma da ICP-Brasil. Ademais não será necessário realizar o processo de verificação por parte do AGR.

NOTA 11*:* Pode ser utilizado para convalidação, caso os dados biográficos não tenham sido alterados, o certificado digital válido do requerente.

2.2.5.6. Caso o resultado da verificação biométrica tenha encontrado o CPF (indexador - IDN) do requerente do certificado digital, com o resultado da comparação "negativo", os AGRs, além de realizarem as validações e verificações elencadas no DOC-ICP-05.02, 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 (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 12: 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 13: 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 (qualidade da impressão digital – processo de coleta elencado no subitem 2.2.1.2). Caso nenhuma impressão digital tenha qualidade para verificação, esse requerente não poderá ser identificado pelo processo da verificação biométrica da impressão digital.

NOTA 14: 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.

2.2.5.7. Caso ocorra qualquer indisponibilidade no Sistema Biométrico da ICP-Brasil, deve-se proceder com as demais verificações obrigatórias exigidas pela ICP-Brasil e, posteriormente, realizar a consulta pendente quando Sistema Biométrico da ICP-Brasil estiver disponível.

2.2.5.8. Antes de inserir as informações do requerente no banco de dados biométrico da ICP-Brasil, os AGR devem realizar todas as validações e verificações dos documentos exigidos, conforme o disposto no subitem 2.2.4., bem como fazer uma análise detalhada, quando o resultado for negativo, principalmente na primeira verificação biométrica (nessa situação deve-se verificar as duas biometrias, impressão digital e face). Caso seja a primeira consulta àquele CPF (indexador), é recomendável disponibilizar um aviso aos AGR para as precauções necessárias referidas neste item. Concluída a análise detalhada da AR e AC no sentido de se emitir o certificado digital ao requerente titular de fato do documento de identificação, é recomendável que conste na base de dados biométrica da ICP-Brasil, um aviso de que aquele registro encontra-se "íntegro e analisado", não sendo mais necessária a revalidação da informação do registro, por parte das AR e AC.

NOTA 15: As medidas estabelecidas neste item buscam resguardar a primeira informação biométrica/biográfica de um requerente/registro contida no banco de dados biométricos da ICP-Brasil. Como as informações biográficas estarão atreladas à informação biométrica, caso o

registro inicial seja de um fraudador e essa mesma pessoa continue requerendo todas as emissões de certificados digitais ICP-Brasil, a fraude só será identificada quando o verdadeiro titular do CPF (indexador) se apresentar para coleta/identificação biométrica.

2.2.5.9. 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.

2.2.6 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 do Sistema de Gestão de Pessoal (SIGEPE), administrado pelo Ministério do Planejamento, Desenvolvimento e Gestão, e dos sistemas correlatos no âmbito dos Comandos Militares;

b) realizar a verificação da solicitação de certificado mediante confirmação dos dados constantes no SIGEPE e nos sistemas correlatos no âmbito dos Comandos Militares, 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;

c) 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, com comprovação auditável do cadastro desses requerentes por parte da AC. Essa comprovação poderá ser pelo CPF ou outro indexador viável entre os sistemas;

d) obter os dados do servidor público federal da ativa e militar da União via sistema indicado pelo Ministério do Planejamento, Desenvolvimento e Gestão e pelos Comandos Militares, sem que haja qualquer possibilidade de alteração desses, para que sejam enviados para a AC emitir o certificado digital;

e) ser assinada por autoridade designada pelo Ministério do Planejamento, Desenvolvimento e Gestão e pelos Comandos Militares, sendo a AC responsável por manter cadastro atualizado das autoridades competentes informados pelo Ministério do Planejamento, Desenvolvimento e Gestão e pelos Comandos Militares e das respectivas autorizações e/ou requisições para fins de auditoria e fiscalização pela AC- Raiz.

2.2.6.1 Módulo Eletrônico da AR do Ministério do Planejamento, Desenvolvimento e Gestão e dos Comandos Militares.

A AR, representada pelo módulo eletrônico da AR do Ministério do Planejamento, Desenvolvimento e Gestão e dos Comandos Militares, 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 armazenado conforme definido do DOC-ICP-05;

c) comunicar diretamente utilizando protocolos de comunicação seguro com os sistemas determinados formalmente pelo Ministério do Planejamento, Desenvolvimento e Gestão, pelos Comandos Militares, pelo Tribunal Superior Eleitoral ou pelo Prestador de Serviço Biométrico;

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 federais, 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. Os autorizadores serão formalmente designados pelos órgãos competentes, por instrumento normativo do Ministério do Planejamento, Desenvolvimento e Gestão ou dos Comandos Militares.

NOTA 15-A: Ficam excepcionalizados para as AR descritas no item 2.2.6.1 os requisitos dispostos no DOC-ICP-03.01.

2.2.6.2 Aplica-se o disposto no item 2.2.6 aos servidores públicos estaduais e do Distrito Federal desde que as Unidades da Federação as quais estejam vinculados:

a) possuam Sistema de Gestão de Pessoal equivalente ao SIGEPE, utilizado na esfera Federal, 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;

c) possuam uma AR credenciada junto a ICP-Brasil e que disponibilize um módulo de AR que atenda aos requisitos previstos no item 2.2.6.1.

2.2.7 A solicitação de certificados digitais para titulares pessoa física de conta de depósitos em Bancos Múltiplos e Caixa Econômica Federal autorizados a funcionar pelo Banco Central do Brasil, deverá seguir o procedimento abaixo descrito:

a) ser dirigida, no formato eletrônico ou físico, aos Bancos Múltiplos ou Caixa Econômica Federal credenciada como AR da ICP-Brasil, ou ainda, aos Bancos Múltiplos ou Caixa Econômica Federal não credenciada que encaminhará à AR da ICP-Brasil contratada para esta finalidade;

b) ser providenciada a verificação, por agente de registro, dos dados do titular pessoa física de conta depósito solicitante do certificado digital;

c) ser providenciada a validação perante agente de registro da solicitação do certificado por meio de processo de identificação inequívoca e presencial do titular pessoa física de conta depósito de Bancos Múltiplos ou Caixa Econômica Federal, com coleta ou verificação biométrica via PSBIO credenciado. O agente de registro que executa a validação deve ser, obrigatoriamente, distinto do agente de registro que executa a verificação.

2.2.7.1Para os Bancos Múltiplos e Caixa Econômica Federal solicitarem a emissão de certificado

digital para titular pessoa física de conta depósito deverá:

I - coletar as informações cadastrais do titular pessoa física de conta depósito de Bancos Múltiplos ou Caixa Econômica Federal exigidas pelo Conselho Monetário Nacional (CMN) e Banco Central do Brasil (BACEN), conforme normativos que regulamentem o processo de identificação e cadastro de Clientes pessoa física para abertura de conta de depósitos, bem como adotar procedimentos contínuos de atualização e adequação das informações coletadas;

II - armazenar em local seguro a ficha-proposta utilizada para a coleta das informações do titular pessoa física de conta depósito, bem como as cópias da respectiva documentação ou registros eletrônicos de conferência, sendo permitida sua microfilmagem ou digitalização, nos termos da regulamentação do BACEN e/ou CMN que estiver em vigor;

III - coletar a biometria facial e impressão digital do titular pessoa física de conta depósito de Bancos Múltiplos ou Caixa Econômica Federal, utilizando padrão adotado pelo PSBIO da ICP-Brasil;

IV – remeter cópia digital dos dados do titular pessoa física de conta depósito de Bancos Múltiplos ou Caixa Econômica Federal à AR de forma segura, quando essa instituição financeira não for credenciada como AR da ICP-Brasil.

2.2.7.2 A AR de Bancos Múltiplos ou Caixa Econômica Federal credenciada na ICP-Brasil deverá ter um módulo eletrônico de AR.

2.2.7.2.1 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 armazenado conforme definido do DOC-ICP-05;

c) comunicar diretamente utilizando protocolos de comunicação seguro com os sistemas determinados formalmente pelosBancos Múltiplos e Caixa Econômica Federal, pela AR (quando aplicável), pela AC e pelo Prestador de Serviço Biométrico (PSBIO);

d) ser auditada pelo ITI em procedimento pré-operacional;

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.

NOTA 15-B: As AR descritas no item 2.2.7.2 ficam dispensadas dos requisitos dispostos no item 2 “Segurança de Pessoal” e item 4.2 “Aplicativo de AR” do DOC-ICP-03.01, para aqueles requisitos equivalentes aos previstos nas normas do Banco Central do Brasil.

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 (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 do comunicado de fraude/indício – 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 16**:* 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, 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 17: 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 todos os AGR 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 18: 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 (Métodos de Interface do Serviço de Lista Negativa).

NOTA 19: Qualquer cancelamento de fraude, feito pelas AC por processos de auditoria e análise detalhada por parte das AR e AC, 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.