

INSTRUÇÃO NORMATIVA ITI N° 05, DE 22 DE FEVEREIRO DE 2021

Aprova a versão 4.0 do DOC-ICP-05.02, aprova a versão 2.0 do DOC-ICP-05.05 e altera o DOC-ICP-05.03 para prever a emissão de certificados digitais por videoconferência.

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

CONSIDERANDO a determinação estabelecida pelo Decreto nº 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 o relatório final do Grupo de Trabalho Técnico instituído pela Portaria nº 049, de 20 de outubro de 2020, do Instituto Nacional de Tecnologia da Informação, com a finalidade de realizar estudos e apresentar proposta de revisão dos atos regulamentares que tratam dos procedimentos e requisitos técnicos para coleta biométrica e cadastro inicial de requerentes de certificados digitais,

RESOLVE:

Art. 1º Esta Instrução Normativa aprova a versão 4.0 do documento “Procedimentos para identificação do requerente e comunicação de irregularidade no processo de emissão de certificado digital” (DOC-ICP-05.02) e a versão 2.0 do documento “Procedimentos para identificação de requerentes de certificados digitais por de videoconferência” (DOC-ICP-05.05).

Art. 2º Esta Instrução Normativa altera o documento “Procedimentos para identificação biométrica na ICP-Brasil DOC-ICP-05.03”, consolidado pela [Instrução Normativa ITI nº 09, de 22 de outubro de 2020](#), para prever a emissão de certificados digitais por videoconferência.

Art. 3º O Anexo da [Instrução Normativa ITI nº 09, de 22 de outubro de 2020](#), (DOC-ICP-05.03) passa a vigorar com as seguintes alterações:

“.....

1 INTRODUÇÃO

O Sistema Biométrico da ICP-Brasil, associado com as verificações em bases oficiais nacionais, tem por objetivo aumentar a segurança na identificação dos titulares e responsáveis por certificados digitais, reduzindo o risco de fraudes, e permitir a simplificação do processo de emissão de certificados digitais através da verificação biométrica do requerente.

1.1

.....

e) transação biométrica: a transação biométrica é um conjunto de dados, em formato eletrônico, contendo dados biométricos e que tem um propósito, como cadastramento, atualização, verificação e identificação. Cada transação no sistema biométrico da ICP-Brasil é identificada por um código único (TCN);

.....

i) bases oficiais nacionais: bases de dados de amplitude nacional e de grande abrangência de cidadãos, que contenham dados biométricos e biográficos, regulamentadas no âmbito da ICP-Brasil para uso na confirmação da identidade de requerentes de certificados digitais.

.....

1.2.....

a) AR: Autoridade de Registro responsável pela identificação do requerente de um certificado digital. Entre outros procedimentos de identificação, deve submeter à AC coleta de uma, sendo obrigatoriamente a face, ou mais biometrias para permitir a validação ou cadastro de uma biometria na Rede PSBio e verificação em base oficial nacional;

b) AC: Autoridade Certificadora responsável pela emissão do certificado digital. No processo de identificação biométrica, tem como responsabilidades principais assegurar a anonimidade das biometrias na Rede PSBio através da associação a um IDN, submissão das biometrias para um PSBio credenciado, verificação biométrica em base oficial nacional e a tomada de providências quando a Rede PSBio indica uma exceção (possível fraude ou erro); e

.....

1.5 Bases Oficiais Nacionais

1.5.1 Conforme estabelecido no DOC-ICP-05 [1], as Bases Oficiais Nacionais admitidas na ICP_Brasil para fins de batimento biométrico e biográfico são as seguintes:

a) base de dados da Identificação Civil Nacional (ICN), mantida pelo Tribunal Superior Eleitoral – TSE; e

b) base de dados do Departamento Nacional de Trânsito – Denatran.

2 COLETA E PROCEDIMENTO BIOMÉTRICOS

2.1 A coleta de dados biométricos na modalidade presencial deve ser feita de forma assistida (acompanhada) por um agente de registro (AGR). Na modalidade remota por videoconferência, a coleta de dados biométricos deverá ser realizada pela captura de face (frame) do requerente durante a videoconferência de forma assistida e, opcionalmente, pela coleta das impressões digitais do requerente de forma não assistida e assíncrona à videoconferência, para execução do batimento biométrico junto a uma base oficial nacional ou PSBio.

.....

2.4.1.....

.....

p).....

.....

iii. a aplicação de videoconferência responsável pela captura da face (frame) deverá efetuar a crítica dos parâmetros dispostos nas alíneas acima.

2.4.2.....

.....

c) área de leitura mínima de 294 mm² para leitores de contato;

.....

e) coleta Batida/Pousada sobre o leitor de contato; ou coleta sem contato, admitida em processo de emissão remota por videoconferência, conforme prevista no item 2.1, acima;

f).....

i. devem ser capturados, por padrão, 4 (quatro) dedos, preferencialmente o médio e o indicador;

.....

iv. será admitida a coleta apenas da face se todos os dedos estiverem marcados como ausentes, amputados ou se emissão por batimento biométrico em base oficial nacional;

.....

.....

2.5.3 A AC deve manter as imagens das biometrias coletadas (impressão digital, face ou ambas) em arquivo, associadas ao IDN e TCN que foi gerado na Rede PSBio.

2.5.4 A AC pode, a seu critério, manter sistema biométrico capaz de realizar operação de verificação (1:1) com o objetivo de fazer uma validação da identificação do requerente antes de submeter à transação de verificação ou atualização ao PSBio ou à base oficial nacional, com objetivo de oferecer um retorno imediato do resultado desta verificação ao AGR.

2.5.4.1 Essa verificação deve ser feita apenas em dados biométricos que tenham sido aprovados pela Rede PSBio ou em base oficial nacional especificada neste documento, devendo a AC garantir a manutenção de sua base local e da rede PSBio, utilizando as aprovações ou rejeições de transações que ocorram no seu PSBio ou nas bases oficiais nacionais.

.....

3.5.2 As exceções (suspeitas de irregularidades e duplicidades dos registros) devem ser prontamente comunicadas para as entidades biométricas credenciadas, se for o caso, disponibilizando essas informações para a AC que solicitou o cadastramento, para os devidos encaminhamentos.

.....

3.6.3.....

.....

d) face para os PSBios: para FAR de 0,1%, TAR de, no mínimo, 90%.

e) face para base do Denatran: para FAR de 0,1%, TAR de, no mínimo, 93%, quando o retorno for disponibilizado por taxa de acurácia.

f) face para base ICN/TSE: retorno de verificação positiva (*true*).

.....

3.8.4 O serviço de consulta de IDN será realizado através de GET no *endpoint* descrito no arquivo *swagger* disponível no Repositório da AC Raiz.

.....

3.8.6 O serviço de listagem de operações pendentes será realizado através de GET no *endpoint* descrito no arquivo *swagger* disponível no Repositório da AC Raiz.

3.8.7 O serviço de requisição de reenvio de operações pendentes será realizado através de POST no *endpoint* descrito no arquivo *swagger* disponível no Repositório da AC Raiz.

.....

3.10.2 O PSBio de destino, ao receber nova versão de uma transação anteriormente recusada, deve utilizar o novo pacote NIST e reprocessar a transação.

.....

4.1.2 Caso o CPF ainda não esteja cadastrado na **Base Local da AC**, deve ser realizada uma coleta de cadastro (ENR), conforme abaixo:

a) na modalidade presencial sem batimento biométrico em base oficial nacional, mantém-se a coleta de face e impressões digitais do requerente, conforme estabelecido neste documento;

b) na modalidade com batimento biométrico em base oficial nacional, admite-se somente a face ou impressões digitais e face do requerente, conforme estabelecido neste documento.

.....

4.1.5 Ao final da coleta, o AGR receberá um relatório da coleta a ser anexado ao dossiê do titular, contendo o TCN enviado à Rede PSBio e, se aplicável, o resultado da verificação local (1:1) na base biométrica local da AC ou da verificação na base oficial nacional.

.....

4.4.4.4 A comparação deve ser realizada através de dedos, para aqueles registros em que isso for possível (existir ao menos um dedo coincidente), e por face, nos registros onde não existirem dedos disponíveis para identificação. No caso de emissão primária com batimento biométrico em base de identificação oficial, fica dispensada essa comparação de face (1:N).

.....

5.1 Tipos de Transações para PSBios

.....

5.2 Formatos de Transações Biométricas para PSBios

.....

5.3 Descrição das Transações para PSBios

.....

5.4 Transações para Bases Oficiais Nacionais

5.4.1 As transações realizadas com bases oficiais nacionais se resumem à transação de verificação (1:1) com o objetivo de fazer uma confirmação dos dados biográficos e biométricos do requerente. Essas transações devem seguir os procedimentos e requisitos estabelecidos pelo serviço de consulta a essas bases.

.....” (NR)

Art. 4º Ficam aprovadas:

- I - a versão 4.0 do documento “DOC-ICP-05.02 – Procedimentos para identificação do requerente e comunicação de irregularidade no processo de emissão de certificado digital”, na forma do Anexo I desta Instrução Normativa;
- II - a versão 2.0 do documento “DOC-ICP-05.05 – Procedimentos para identificação de requerentes de certificados digitais por de videoconferência”, na forma do Anexo II desta Instrução Normativa; e
- III - a versão 3.0 do documento “DOC-ICP 05.03 – Procedimentos para identificação biométrica na ICP-Brasil”.

Parágrafo único. A identificação da versão do documento “Procedimentos para identificação biométrica na ICP-Brasil” deverá ser alterada no preâmbulo e incluída no controle de versões do anexo da [Instrução Normativa ITI nº 09, de 22 de outubro de 2020](#).

Art. 5º Ficam revogadas:

I - a [Instrução Normativa ITI nº 12, de 26 de outubro de 2020](#); e

II - a [Instrução Normativa nº 02, de 20 de março de 2020](#).

Art. 6º Esta Instrução Normativa entra em vigor em 1º de março de 2021.

CARLOS ROBERTO FORTNER



Infraestrutura de Chaves Públicas Brasileira

ANEXO I

PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL

DOC-ICP-05.02

Versão 4.0

22 de fevereiro de 2021



Infraestrutura de Chaves Públicas Brasileira

SUMÁRIO

CONTROLE DE ALTERAÇÕES.....	3
LISTA DE SIGLAS E ACRÔNIMOS	5
1 DISPOSIÇÕES GERAIS	6
2 PROCEDIMENTO PARA CONFIRMAÇÃO DA IDENTIDADE DO REQUERENTE ..	7
3 COMUNICAÇÃO DE UMA OCORRÊNCIA DE FRAUDE OU INDÍCIO	10
4 DOCUMENTOS REFERENCIADOS.....	14



Infraestrutura de Chaves Públicas Brasileira

CONTROLE DE ALTERAÇÕES

Ato que aprovou a alteração	Item alterado	Descrição da alteração
Instrução Normativa ITI nº 05, de 22.02.2021 Versão 4.0		Adequação à emissão primária por videoconferência.
Instrução Normativa nº 12, de 26.10.2020 Versão 3.0		Revisão e consolidação do DOC-ICP-05.02 conforme Decreto nº 10.139, de 28 de novembro de 2019. Adequação à emissão de certificado de forma não presencial.
Resolução nº 151 de 30.05.2019 Versão 2.0	1, 2, 3, e 4	Simplificação dos Processos da ICP-Brasil.
Instrução Normativa nº 04, de 30.04.2019 Versão 1.8	2.2.6	Trata da solicitação de certificado para servidores públicos federais da ativa e militares da união.
Resolução nº 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 <i>Subject Alternative Name</i> .
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.



Infraestrutura de Chaves Públicas Brasileira

Ato que aprovou a alteração	Item alterado	Descrição da alteração
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.



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridade de Registro
AGR	Agente de Registro
CNAE	Classificação Nacional de Atividades Econômicas
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro Nacional de Pessoa Física
CTPS	Carteira de Trabalho e Previdência Social
DAFN	Diretoria de Auditoria, Fiscalização e Normalização
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



Infraestrutura de Chaves Públicas Brasileira

1 DISPOSIÇÕES GERAIS

1.1 Este documento se aplica ao processo de identificação do requerente de certificado digital, bem como das comunicações de eventuais tentativas de fraudes e irregularidades na emissão de um certificado digital ICP-Brasil.

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

- a) Agente de registro (AGR) – Pessoa responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a identificação do requerente quando da solicitação de certificados.
- b) Autoridade de registro – AR - Entidade responsável pela interface entre o usuário e a Autoridade Certificadora – AC. É sempre vinculada a uma AC e tem por objetivo o recebimento e o encaminhamento de solicitações de emissão ou revogação de certificados digitais às ACs e a identificação, 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) Emissão do certificado – Conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.
- f) Identificação do requerente de certificado – Compreende 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.
- g) Ponto de Centralização da AC – Local único, em território nacional, onde a AC armazena os dossiês de todos os Agentes de Registro das ARs vinculadas. Deve armazenar os dossiês eletrônicos de titulares de certificados da ICP-Brasil e deve armazenar eletronicamente os documentos de identificação, fotografia da face e impressões digitais do requerente.
- h) Lista Negativa – Conjunto de informações derivadas dos comunicados de fraude, ou indícios de fraude, feitos pelas ACs (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.



Infraestrutura de Chaves Públicas Brasileira

- i) Sistema Biométrico ICP-Brasil – Sistema composto pelos Prestadores de Serviço Biométrico - PSBio, credenciados pelo ITI, responsáveis pela identificação (1:N) biométrica (que formará um registro/requerente único em um ou mais bancos/sistemas de dados biométrico para toda ICP-Brasil), bem como pela verificação (1:1) biométrica do requerente de um certificado digital (que trata da comparação entre uma biometria, que possua característica perene e unívoca, de acordo com os padrões internacionais de uso, como, por exemplo, impressão digital, face, íris, voz, coletada no processo de emissão do certificado digital com outra já armazenada em bancos/sistemas de dados biométrico da ICP-Brasil relativa ao mesmo requerente registro/indexador).
- j) Bases Oficiais Nacionais – Bases de dados de amplitude nacional e de grande abrangência de cidadãos, que contenham dados biométricos e biográficos, regulamentadas no âmbito da ICP-Brasil para uso na confirmação da identidade de requerentes de certificados digitais.

2 PROCEDIMENTO PARA CONFIRMAÇÃO DA IDENTIDADE DO REQUERENTE

2.1 As ACs devem definir em suas DPCs os procedimentos empregados pelas suas ARs vinculadas para a confirmação da identidade de um indivíduo, observado o disposto no DOC-ICP-05 [1].

2.1.1 Essa confirmação deverá ser realizada com base nos documentos e procedimentos de identificação definidos no DOC-ICP-05 [1], em uma das formas admitidas na ICP-Brasil:

- a) mediante comparecimento presencial;
- b) por videoconferência; ou
- c) com uso de certificado ICP-Brasil válido.

2.1.2 A confirmação de identidade do requerente do certificado digital deve compreender, no mínimo, os seguintes aspectos:

- a) Apresentação e verificação da documentação exigida;
- b) Coleta e verificação biométrica; e
- c) Consulta à base de dados da Lista Negativa de ACs.

2.1.3 A coleta e a verificação biométrica do requerente deverão seguir os procedimentos para coleta e identificação biométrica na ICP-Brasil definidos no DOC-ICP-05.03 [3].

2.1.4 A confirmação da identidade realizada por meio de videoconferência deve seguir os procedimentos de identificação do requerente dispostos no DOC-ICP-05.05 [8].



Infraestrutura de Chaves Públicas Brasileira

2.1.5 É dispensada a apresentação dos documentos da pessoa física requerente, ou do responsável pelo certificado da pessoa jurídica, quando houver a identificação positiva junto ao Sistema Biométrico da ICP-Brasil, exceto quando houver alteração de dados ou a necessidade de complementar a documentação, conforme disposto no item 2.3.5.

2.1.6 Os procedimentos de comprovação de identidade de que trata esse DOC não se aplicam na hipótese de emissão de certificados de pessoas físicas, caso a solicitação seja assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e cujos dados biométricos já tenham sido devidamente coletados.

2.1.7 No caso de certificados de pessoas jurídicas, fica dispensada a apresentação dos documentos da pessoa física responsável, bem como a coleta e verificação dos seus dados biométricos, nas seguintes hipóteses:

- a) quando a solicitação for assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, de mesma titularidade e responsável, e cujos dados biométricos deste último tenham sido devidamente coletados; ou
- b) quando a solicitação for assinada com certificado digital ICP-Brasil válido, do tipo A3 ou superior, cuja titularidade seja da mesma pessoa física responsável legal da organização e a verificação dos documentos pertinentes à pessoa jurídica possa ser realizada eletronicamente, por meio de barramento ou aplicação oficial.

2.1.7.1 O disposto neste item não afasta a necessidade de apresentação dos documentos pertinentes à pessoa jurídica requerente, ou os demais requisitos exigidos para identificação da requerente.

2.2 As ACs devem disponibilizar, para todas as ARs vinculadas às suas respectivas cadeias, uma interface para consulta às suas bases de dados da Lista Negativa das ACs, com requisitos de segurança e disponibilidade, conforme ADE-ICP-05.02.B [2], durante o processo de identificação de requerente de um certificado digital ICP-Brasil.

2.2.1 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 [2] (Métodos de Interface do Serviço de Lista Negativa).

2.2.2 Ao consultar a Lista Negativa, com o objetivo de identificar possíveis fraudadores, o AGR deverá confrontar as informações biográficas dos documentos de identificação apresentados, a imagem da face, as impressões digitais, quando houver, e as características fisiológicas da pessoa física que a ele se apresenta para identificação, bem como, as informações dos documentos de constituição da pessoa jurídica, quando for caso, com aquelas que constam registradas na Lista Negativa.

2.2.3 Realizada a consulta à Lista Negativa da AC, deverão ser adotadas as seguintes providências:

2.2.3.1 No caso de concluir tratar-se de tentativa de fraude, o certificado não deve ser emitido, e a AR deve comunicar à AC, que por sua vez deve comunicar ao ITI a tentativa de fraude, conforme disposto do item 3.



Infraestrutura de Chaves Públicas Brasileira

2.2.3.2 No caso de concluir que o registro de tentativa ou de fraude constante da Lista Negativa seja indevido, o certificado pode ser emitido e a AC deve solicitar o cancelamento do respectivo registro de tentativa ou de fraude na Lista Negativa, embasando detalhadamente os motivos de tal conclusão, conforme disposto no item 3.

2.2.3.3 No caso de não haver qualquer intercorrência na consulta e confrontação dos dados das Listas Negativas, de modo que se conclua não tratar-se de tentativa de fraude, a AR deve dar prosseguimento aos demais procedimentos de identificação para emissão do certificado.

2.3 As ACs devem disponibilizar, para todas as ARs vinculadas à sua respectiva cadeia, uma interface para coleta, verificação e identificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil e às Bases Oficiais Nacionais, em cada processo de emissão de um certificado digital ICP-Brasil, podendo ser coletada ou verificada a biometria uma única vez para o mesmo titular de vários certificados no ato de identificação.

2.3.1 A interface da aplicação para os AGRs deve possibilitar consulta pelo CPF (indexador) do requerente do certificado digital, com a coleta, no mínimo, de uma biometria (digital, facial ou ambas), preferencialmente a que possuir melhor qualidade do requerente no processo de emissão do certificado digital, a qual deverá ser enviada/comparada obrigatoriamente com o registro daquela biometria específica no Sistema de Dados Biométricos da ICP-Brasil ou em Bases Oficiais Nacionais.

2.3.1.1 É recomendável que o Sistema Biométrico da ICP-Brasil informe ao AGR qual é o “melhor dedo”, no caso de verificação da biometria da impressão digital. Caso nenhuma impressão digital tenha qualidade para verificação, esse requerente não poderá ser identificado pelo processo da verificação biométrica da impressão digital.

2.3.1.2 Considerando que o Sistema Biométrico da ICP-Brasil deve ser capaz de verificar a biometria da impressão digital e da face do requerente, quando não houver possibilidade de utilização da impressão digital, deve-se utilizar a biometria da face.

2.3.2 Caso o CPF (indexador) não conste na base de dados biométrica da ICP-Brasil ou nas Bases Oficiais Nacionais, tal fato deve ser informado ao AGR, hipótese em que deverá ser realizada a coleta dos dados biográficos e biométricos do requerente, na forma disposta no DOC ICP 05.03, bem como adotar as demais providências para confirmação da identidade.

2.3.3 Caso o CPF (indexador) esteja no banco/sistema de dados biométricos da ICP-Brasil ou nas bases oficiais nacionais, a consulta deve indicar um resultado “positivo” (biometria comparada pertence de fato ao requerente), ou “negativo” (biometria comparada não pertence ao requerente ou resultou em um erro).

2.3.3.1 O resultado “positivo” da consulta à base de dados biométrica significa que obteve o atingimento pleno da taxa de aceitação da acurácia estabelecida no DOC-ICP-05.03 [3]. Resultado negativo, ao contrário, significa que não se obteve o atingimento da taxa de aceitação.

2.3.4 O resultado “positivo” da consulta à base de dados biométrica da ICP-Brasil ou em Bases Oficiais nacionais deve ser apensado ao dossiê do titular do certificado e preservados de acordo com o DOC-ICP-03.01 [7].



Infraestrutura de Chaves Públicas Brasileira

2.3.5 Caso o resultado da verificação biométrica no Sistema Biométrico da ICP-Brasil tenha encontrado CPF (indexador) do requerente do certificado digital, com o resultado “positivo”, fica dispensada a apresentação e verificação dos documentos de identificação do requerente pessoa física ou do responsável pelo certificado da pessoa jurídica, previstos no DOC ICP 05 .

2.3.6 Caso o resultado da verificação biométrica no Sistema Biométrico da ICP-Brasil tenha encontrado o CPF (indexador - IDN) do requerente do certificado digital, com o resultado da comparação “negativo”, deve-se comunicar à AC vinculada para que se faça uma análise detalhada do caso.

2.3.6.1 Se a AR ou a AC, após a análise, concluíam 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, com a análise dos demais requisitos exigidos.

2.3.6.2 Na hipótese do registro biométrico e/ou biográfico ter sido armazenado no banco de dados de forma irregular, tanto da AC, quanto do respectivo Sistema Biométrico (PSBio) credenciado na ICP-Brasil, as ACs devem realizar os procedimentos mencionados no DOC-ICP-05.03 [3] (notificação de irregularidade do registro).

2.3.6.3 Concluindo a AR ou a AC se tratar de tentativa de fraude, deverá ser feita a comunicação ao ITI, conforme item 3.

2.3.6.4 Não necessariamente um resultado negativo indica uma tentativa de fraude e/ou que o registro do requerente armazenado no banco de dados biométricos seja de um suposto fraudador. Em alguns casos, por algum processo de deterioração ou transformação (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.

2.3.7 Caso ocorra qualquer indisponibilidade no Sistema Biométrico da ICP-Brasil, deve-se proceder com a verificação obrigatória exigida pela ICP-Brasil e, posteriormente, realizar a consulta pendente quando Sistema Biométrico da ICP-Brasil estiver disponível.

2.3.8 Todos os logs de transação biométrica feitos pelo AGR devem ser guardados pelo período mínimo de 7 anos pelas ACs, conforme disposto no DOC-ICP-05 [1].

2.4 Os resultados, sem irregularidades, da consulta e confirmação da identificação do requerente de um certificado deverão ser arquivados ao dossiê eletrônico do titular.

2.4.1 As ACs devem manter os arquivos de imagem de todos os dados biométricos coletados de um requerente durante o processo de identificação associados ao dossiê do requerente do certificado digital.

3 COMUNICAÇÃO DE UMA OCORRÊNCIA DE FRAUDE OU INDÍCIO

3.1 Quando a AR ou a AC concluir ter ocorrido fraude ou tentativa de fraude na emissão de certificados digitais, deverão comunicar tal fato ao ITI, mediante o procedimento descrito neste item.

3.2 A comunicação de fraude ou tentativa de fraude deverá ser realizado por meio do preenchimento dos seguintes campos na interface do sistema de comunicação de fraude da AC, determinado no método descrito no adendo referente aos Métodos de Interface do Serviço de Lista Negativa [2], a ser encaminhado ao ITI:

- a) 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);
- b) Nome do Informante: quem está cadastrando a fraude – opcional;
- c) CPF do Informante: CPF de quem está cadastrando a fraude – opcional;
- d) UF: escolha da UF onde ocorreu a fraude/indício (tabela pré-determinada) – obrigatório;
- e) Município: escolha do município onde ocorreu a fraude/indício (tabela pré-determinada por UF) – obrigatório;
- f) Tipo de Ocorrência: indício ou fraude – obrigatório;
- g) Número do certificado: número de série do certificado se for fraude – obrigatório;
- h) 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;
- i) Data da ocorrência: data da identificação do indivíduo – obrigatório;
- j) Diligência de investigação: como foi detectada a fraude. 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;
- k) Nome: nome conforme aparece no documento apresentado – obrigatório;
- l) CPF: número do CPF conforme apresentado no documento – obrigatório;
- m) Data de nascimento: data conforme apresentado no documento – obrigatório;
- n) Correio eletrônico: correio eletrônico fornecido do suposto fraudador – opcional;
- o) Telefone: telefone fornecido do suposto cliente – opcional;
- p) Documento de identidade: deverá ser informado o número e a data de expedição do respectivo documento e, sempre que constante do documento, o número do RG – obrigatório, se for o caso;
- q) Certidão: certidões depois de 2009 apresentam uma matrícula (número único), que deve ser colocada no campo “número”. Fornecer as seguintes informações, quando constantes da certidão: (i) número; (ii) naturalidade ; (iii) livro; (iv) folha; (v) número de RG, CTPS, quando presentes – opcional;



Infraestrutura de Chaves Públicas Brasileira

- r) CNH: caso seja CNH apresentada, fornecer as seguintes informações: (i) número; (ii) data de emissão; (iii) 1ª habilitação; (iv) UF expedição; (v) data de validade; (vi). formulário; (vii) número de identidade – obrigatório, se for o caso;
- s) Passaporte: caso seja Passaporte apresentado, fornecer as seguintes informações: (i) número; (ii) data de expedição; (iii) data de validade; (iv) país (tabela pré-determinada) – obrigatório, se for o caso;
- t) CTPS: caso seja CTPS apresentada, fornecer as seguintes informações: (i) número; (ii) data de emissão; (iii) PIS/PASEP; (iv) UF (tabela pré-determinada) – obrigatório, se for o caso;
- u) 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: (i) número; (ii) data de emissão; (iii) nome; (iv) UF (tabela pré-determinada) – obrigatório, se for o caso;
- v) Características físicas: devem ser selecionadas as características físicas perceptíveis do suposto fraudador, tais quais: (i) cor da pele (seleção: amarelo; branco; indígena; negro; pardo); (ii) cor dos olhos (seleção: claros; escuros); (iii) cor predominante do cabelo (seleção: branco; escuro; grisalho; loiro; ruivo); (iv) deficiências físicas perceptíveis (seleção: cadeirante; cego; manco; mudo; surdo); (v) idade aparente (seleção: A – menor que 30 anos; B – entre 30 e 50 anos; C – mais de 50 anos); (vi). sexo (seleção: masculino; feminino); (vii) 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); (viii) tipo de cabelo (seleção: calvo; curto; longo; médio) – opcional;
- w) Informações da empresa: fornecer as seguintes informações: (i) CNPJ; (ii) razão social; (iii) endereço; (iv) telefone; (v) CEP; (vi) CNAE; (vii) UF (tabela pré-determinada); (viii) Município (tabela pré-determinada por UF) – obrigatório, se for o caso;
- x) 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;

3.2.1 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 [3], 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.



Infraestrutura de Chaves Públicas Brasileira

3.2.2 Deve se ter certeza da informação antes de adicionar as características físicas do fraudador. Em caso de dúvida, deve-se deixar uma ou mais informações físicas sem serem adicionadas. Como essas informações serão utilizadas posteriormente por todas as ACs para as pesquisas por características físicas na Lista Negativa da AC, é fundamental que estejam corretas para que se tornem eficientes.

3.2.3 A imagem do documento de identificação deverá ser juntada 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).

3.3 Após 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 [2].

3.4 Qualquer cancelamento de fraude, feito pelas ACs por processos de auditoria e análise detalhada devem ser enviadas ao endereço de correio eletrônico: comunicafraude@iti.gov.br, com a descrição detalhada dos motivos do cancelamento.

3.5 A AC emissora do certificado digital deve notificar, ou cuidar para que se notifique, a autoridade policial competente mais próxima do ocorrido, a fraude em sua emissão.

3.6 Após o registro na Lista Negativa, o dossiê de emissão do certificado, os dossiês dos AGR que atuaram na identificação e a cópia do Boletim de Ocorrência deverão ser encaminhados ao ITI, aos cuidados da Diretoria de Auditoria, Fiscalização e Normalização – DAFN.



Infraestrutura de Chaves Públicas Brasileira

4 DOCUMENTOS REFERENCIADOS

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL Aprovado pela Resolução nº 42, de 18 de abril de 2006	DOC-ICP-05
[4]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 40, de 18 de abril de 2006	DOC-ICP-03
[5]	CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 28 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

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[3]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL Aprovado pela Resolução nº 114, de 30 de setembro de 2015	DOC-ICP-05.03
[7]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL Aprovado pela Resolução nº 07, de 19 de maio de 2006	DOC-ICP-03.01
[8]	PROCEDIMENTOS PARA IDENTIFICAÇÃO DE REQUERENTES DE CERTIFICADOS DIGITAIS POR VIDEOCONFERÊNCIA Aprovado pela Instrução Normativa nº 02, de 20 de março de 2020	DOC-ICP-05.05



Infraestrutura de Chaves Públicas Brasileira

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

REF.	NOME DO DOCUMENTO	CÓDIGO
[2]	MÉTODOS DE INTERFACE DO SERVIÇO DE LISTA NEGATIVA	ADE-ICP-05.02.B