



**Infraestrutura de Chaves Públicas Brasileira**

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

**DOC-ICP-05.02**

**Versão 2.0**

**30 de maio de 2019**



# Infraestrutura de Chaves Públicas Brasileira

## SUMÁRIO

CONTROLE DE ALTERAÇÕES.....	3
LISTA DE SIGLAS E ACRÔNIMOS.....	4
1 DISPOSIÇÕES GERAIS.....	5
2 VERIFICAÇÃO DA IDENTIDADE DO REQUERENTE.....	6
3 COMUNICAÇÃO DE UMA OCORRÊNCIA DE FRAUDE OU INDÍCIO.....	8
4 DOCUMENTOS REFERENCIADOS.....	12



## Infraestrutura de Chaves Públicas Brasileira

### CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
Resolução nº 151 de 30.05.2019 (Versão 2.0)	1, 2, 3, e 4	Simplificação dos Processos da ICP-Brasil.
Instrução Normativa nº 04, de 30.04.2019 (Versão 1.8)	2.2.6	Trata da solicitação de certificado para servidores públicos federais da ativa e militares da união.
Resolução 141 de 03.07.2018 (Versão 1.7)	2.2.6.2	Incluir os servidores públicos dos estados e do Distrito Federal nos procedimentos específicos de emissão de certificados digitais.
Resolução nº 131, de 10.11.2017 (Versão 1.6)	2.2.1, 2.2.3 e 2.2.7	Identificação de titulares de contas de depósito e validade da CNH.
Resolução nº 128, de 13.09.2017 (Versão 1.5)	2.2.1.c	Esclarece a obrigatoriedade de validação das informações contidas no <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.
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
CNE	Carteira Nacional de Estrangeiro
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro Nacional de Pessoa Física
CTPS	Carteira de Trabalho e Previdência Social
DPC	Declarações de Práticas de Certificação
IBGE	Instituto Brasileiro de Geografia e Estatística
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
PIS/PASEP	Programa de Integração Social/Programa de Formação do Patrimônio do Servidor Público
RG	Registro Geral
UF	Unidade Federativa

## 1 DISPOSIÇÕES GERAIS

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

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

- a) Agente de registro (AGR) – Pessoa responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a identificação do requerente quando da solicitação de certificados.
- b) Autoridade de registro – AR - Entidade responsável pela interface entre o usuário e a Autoridade Certificadora – AC. É sempre vinculada a uma AC e tem por objetivo o recebimento e encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes.
- c) Confirmação da identidade de um indivíduo – Comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada.
- d) Confirmação da identidade de uma organização – Comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição.
- e) Emissão do certificado – Conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.
- f) identificação do requerente de certificado – Compreende na etapa de confirmação da identidade de um indivíduo ou de uma organização, realizadas mediante a presença física do interessado, com base nos documentos de identificação e/ou identificação biométrica, e a etapa de emissão do certificado.
- g) Ponto de Centralização da AC – Local único, em território nacional, onde a AC armazena os dossiês de todos os Agentes de Registro das AR vinculadas. Deve armazenar os dossiês eletrônicos de titulares de certificados da ICP-Brasil e deve armazenar eletronicamente os documentos de identificação, fotografia da face e impressões digitais do requerente.
- h) Lista Negativa – Conjunto de informações derivadas dos comunicados de fraude, ou indícios de fraude, feitos pelas AC (ou pelo próprio ITI por meio de



## Infraestrutura de Chaves Públicas Brasileira

auditoria/fiscalização) da ICP-Brasil ao ITI, em que contém o modo de operação da ocorrência, as informações biográficas do documento apresentado e, se for o caso, das informações sobre a empresa, características fisiológicas do suposto fraudador, a imagem da face e do documento de identificação utilizado pelo suposto fraudador.

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

## 2 VERIFICAÇÃO DA IDENTIDADE DO REQUERENTE

2.1 Conforme estabelecido no DOC-ICP-05 [1], as AC definem em suas DPC os procedimentos empregados pelas suas AR vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e/ou pelo processo de identificação biométrica ICP-Brasil.

2.2 Caso o interessado, pessoa física, já tenha dossiê identificado pela AR, não será necessário nova apresentação dos documentos, exceto quando houver alteração de dados ou a necessidade de complementar a documentação.

2.3 Os resultados, sem irregularidades, da consulta/validação da identificação do requerente de um certificado deverão ser apensados ao dossiê eletrônico do titular.

2.4 As AC devem possuir uma interface para consulta a base de dados da Lista Negativa das ACs, com requisitos de segurança e disponibilidade, nos processos de conferência do documento em papel de emissão de um certificado digital ICP-Brasil.

2.4.1 Essa base de dados da Lista Negativa da AC deve ser atualizada pela comunicação entre o servidor da AC e o servidor do ITI, conforme disposto no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa).

2.4.2 Caso a AR e/ou a AC concluam pela não emissão do certificado digital, a AR, se for o caso, deve comunicar a AC, e essa deve comunicar a tentativa de fraude ao ITI, conforme disposto do item 3. Caso a AR e/ou a AC concluam pela emissão do certificado digital, a AC deve solicitar o cancelamento de fraude, ou tentativa, na Lista Negativa, embasando detalhadamente os motivos de tal, conforme disposto no item 3.



## Infraestrutura de Chaves Públicas Brasileira

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

2.5.1 O Prestador de Serviço Biométrico – PSBio – da ICP-Brasil, que proverá os componentes do sistema biométrico, deve operar e ser credenciado, auditado e fiscalizado, conforme o disposto nos DOC-ICP-05.03 [6], DOC-ICP-03 [2], DOC-ICP-08 [3] e DOC-ICP-09 [4].

2.5.2 A interface da aplicação para os AGR deve disponibilizar, no mínimo, uma consulta pelo CPF (indexador) do requerente do certificado digital, com a coleta de uma biometria (por exemplo, uma impressão digital – preferencialmente a que possui melhor qualidade – e/ou face) do mesmo no processo de emissão do certificado digital, que deve ser enviada/comparada obrigatoriamente com o registro daquela biometria específica do requerente em um banco/sistema de dados biométricos credenciado da ICP-Brasil. Caso o CPF (indexador) esteja no banco/sistema de dados biométricos da ICP-Brasil, a consulta deve indicar um resultado “positivo” (biometria comparada pertence de fato ao requerente, apresentando também, no mínimo, a face e o nome do requerente para o AGR), ou “negativo” (biometria comparada não pertence ao requerente ou resultou em um erro). Caso o CPF (indexador) não conste na base de dados biométrica da ICP-Brasil, tal fato deve ser informado ao AGR.

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

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

**NOTA 2:** Devem ser coletadas as informações biográficas e biométricas, esta última conforme DOC-ICP-05.03 [6] a serem enviadas para AC e, posteriormente enviados ao PSBio.

**NOTA 3:** Um Sistema Biométrico da ICP-Brasil credenciado deve reportar aos outros sistemas biométricos da ICP-Brasil credenciados, se for o caso, e às AC qualquer irregularidade ou duplicidade relativa ao armazenamento biométrico/biográfico de um registro detectada no processo de emissão de um certificado digital, para que as AC solicitantes do cadastro irregular providenciem, se for o caso, a revogação do certificado digital e a comunicação de eventual fraude.

2.5.4 Caso o resultado da verificação biométrica tenha encontrado CPF (indexador) do requerente do certificado digital, com o resultado “positivo”, não será necessária a validação de qualquer documento elencado no item “Documentos para efeitos de identificação de um indivíduo” do DOC-ICP-05 [1].

2.5.5 Caso o resultado da verificação biométrica tenha encontrado o CPF (indexador - IDN) do requerente do certificado digital, com o resultado da comparação “negativo”, devem comunicar à AC vinculada para que se faça uma análise detalhada do caso. Caso a AR e/ou a AC conclua

que o requerente se trata do titular de fato do documento de identificação e/ou das informações da empresa, deverá ser dado prosseguimento ao processo de emissão do certificado digital. O registro biométrico/biográfico armazenado no banco de dados de forma irregular, tanto da AC quanto do respectivo Sistema Biométrico credenciado devem realizar os procedimentos mencionados no DOC-ICP-05.03 [6] (notificação de irregularidade do registro), comunicando ao ITI sobre a fraude. Caso a AR e/ou a AC conclua(m) que o requerente se trata de um suposto fraudador, não deverá ser emitido o certificado digital e a AC deve comunicar a tentativa de fraude ao ITI.

**NOTA 4:** Não necessariamente um resultado negativo indica uma tentativa de fraude e/ou que o registro do requerente armazenado no banco de dados biométricos seja de um suposto fraudador. Em alguns casos, por algum processo de deterioração (temporário ou permanente), pode não ser possível verificar a biometria no processo de emissão do certificado digital, sem que o requerente se trate de um suposto fraudador.

**NOTA 5:** É recomendável que o Sistema Biométrico da ICP-Brasil informe ao AGR qual é o “melhor dedo”, no caso de verificação da biometria da impressão digital. Caso nenhuma impressão digital tenha qualidade para verificação, esse requerente não poderá ser identificado pelo processo da verificação biométrica da impressão digital.

**NOTA 6:** Considerando que o Sistema Biométrico da ICP-Brasil deve ser capaz de verificar, no mínimo, a biometria da impressão digital e da face do requerente, quando não houver possibilidade de utilização da impressão digital, deve-se utilizar outra biometria disponível.

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

2.5.7 As AC devem manter os arquivos de imagem de todos os dados biométricos coletados de um requerente (que já passaram pelo processo de 1:N no Sistema Biométrico da ICP-Brasil) durante o processo de cadastramento, associados ao dossiê do requerente do certificado digital.

### **3 COMUNICAÇÃO DE UMA OCORRÊNCIA DE FRAUDE OU INDÍCIO**

3.1 O sistema de comunicado de fraude ao ITI passa a ser implementado por meio do preenchimento das informações na interface do sistema de comunicação de fraude da AC, determinado no método descrito no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa). Devem ser preenchidos os seguintes campos na interface do sistema pela AC e, posteriormente, enviados ao ITI:

- i. A AC e AR onde ocorreu a fraude ou tentativa (tabela pré-determinada) – obrigatório (lembrando que essas informações não serão replicadas no método de atualização de base da AC, somente serão armazenadas no servidor ITI);
- ii. Nome do Informante: quem está cadastrando a fraude – opcional;





## Infraestrutura de Chaves Públicas Brasileira

- iii. CPF do Informante: CPF de quem está cadastrando a fraude – opcional;
- iv. UF: escolha da UF onde ocorreu a fraude/indício (tabela pré-determinada) – obrigatório;
- v. Município: escolha do município onde ocorreu a fraude/indício (tabela pré-determinada por UF) – obrigatório;
- vi. Tipo de Ocorrência: indício ou fraude – obrigatório;
- vii. Número do certificado: número de série do certificado se for fraude – obrigatório;
- viii. Ocorrência: breve relato do modo de operação do estelionatário, data, tipo de documento apresentado, tipo de certificado fraudado, como foi detectada a fraude/indício (2000 caracteres no máximo) – obrigatório;
- ix. Data da ocorrência: data da identificação do indivíduo – obrigatório;
- x. Diligência de investigação: como foi detectada a fraude (análise do documento). Caso alguma forma de detecção tenha dado como válido o documento, marcar “válido”. Caso a forma de detecção tenha constatado a fraude no documento, marcar como “inválido”. Clicar em “Adicionar” para inclusão – opcional;
- xi. Nome: nome conforme aparece no documento apresentado – obrigatório;
- xii. CPF: número do CPF conforme apresentado no documento – obrigatório;
- xiii. Data de nascimento: data conforme apresentado no documento – obrigatório;
- xiv. Correio eletrônico: correio eletrônico fornecido do suposto fraudador – opcional;
- xv. Telefone: telefone fornecido do suposto cliente – opcional;
- xvi. Documento de identidade: caso seja RG/Carteira militar apresentada pelo requerente, fornecer as seguintes informações, caso apareçam no documento: a. número (mesmo apresentando outro tipo de documento que não seja o RG, como, por exemplo, a CNH, escrever o número de identidade que aparece no documento apresentado); b. Data de expedição; c. – obrigatório, se for o caso;
- xvii. Certidão: certidões depois de 2009 apresentam uma matrícula (número único), que deve ser colocada no campo “número”. Fornecer as informações: a. número (e naturalidade); b. livro; c. folha, caso apareçam no documento (RG, CTPS ou outro) – opcional;
- xviii. CNH: caso seja CNH apresentada, fornecer as seguintes informações: a. número; b. data de emissão; c. 1ª habilitação; d. UF expedição; e. data de validade; f. formulário; g. número de identidade – obrigatório, se for o caso;
- xix. Passaporte: caso seja Passaporte apresentado, fornecer as seguintes informações: a. número; b. data de expedição; c. data de validade; d. país (tabela pré-determinada) – obrigatório, se for o caso;



## Infraestrutura de Chaves Públicas Brasileira

- xx. CTPS: caso seja CTPS apresentada, fornecer as seguintes informações: a. número; b. data de emissão; c. PIS/PASEP; d. UF (tabela pré-determinada) – obrigatório, se for o caso;
- xxi. Outro documento: qualquer outro documento de natureza civil, como, por exemplo, carteira de entidade de classe, que têm por força legal a presunção de identificação, fornecer as seguintes informações: a. número; b. data de emissão; c. nome; d. UF (tabela pré-determinada) – obrigatório, se for o caso;

**NOTA 7:** No campo “outros” do Sistema de Comunicação de Fraude, deve-se, também, realizar o *upload* das imagens em formato WSQ, conforme especificações contidas no DOC-ICP-05.03 [6], das impressões digitais dos supostos fraudadores. Esses arquivos de impressões digitais devem estar nomeados da seguinte forma: 1: Polegar esquerdo; 2: Indicador esquerdo; 3: Dedo médio esquerdo; 4: Anelar esquerdo; 5: Dedo mínimo esquerdo; 6: Polegar direito; 7: Indicador direito; 8: Dedo médio direito; 9: Anelar direito; 10: Dedo mínimo direito. Essas impressões digitais, assim como a face, devem ser submetidas/enviadas pela AC/PSS ao seu respectivo Sistema Biométrico para inserção dessas biometrias no repositório de Lista Negativa biométrica do mesmo.

- xxii. Características físicas: devem ser selecionadas as características físicas perceptíveis do suposto fraudador, tais quais: a. cor da pele (seleção: amarelo; branco; indígena; negro; pardo); b. cor dos olhos (seleção: claros; escuros); c. cor predominante do cabelo (seleção: branco; escuro; grisalho; loiro; ruivo); d. deficiências físicas perceptíveis (seleção: cadeirante; cego; manco; mudo; surdo); e. idade aparente (seleção: A – menor que 30 anos; B – entre 30 e 50 anos; C – mais de 50 anos); f. sexo (seleção: masculino; feminino); g. sinais corporais perceptíveis (seleção: falta de dedos nas mãos; mancha na pele; marcas como cicatrizes; tatuagem ou sinais em membros superiores; tatuagem ou sinais no rosto ou pescoço); h. tipo de cabelo (seleção: calvo; curto; longo; médio) – opcional;

**NOTA 8:** Deve se ter certeza da informação antes de adicionar as características físicas do fraudador. Em caso de dúvida, deve-se deixar uma ou mais informações físicas sem serem adicionadas. Como essas informações serão utilizadas posteriormente por todas as ACs para as pesquisas por características físicas na Lista Negativa da AC, é fundamental que estejam corretas para que se tornem eficientes.

- xxiii. Informações da empresa: fornecer as seguintes informações: a. CNPJ; b. razão social; c. endereço; d. telefone; e. CEP; f. CNAE; g. UF (tabela pré-determinada); h. Município (tabela pré-determinada por UF) – obrigatório, se for o caso;
- xxiv. *Upload* da imagem do documento de identificação e da face: deve ser enviado a imagem do documento de identificação (escolher tipos: RG, CNH, CTPS, PASSAPORTE, OUTROS) e da face (escolher o tipo FOTO) disposta em pé do suposto fraudador no comunicado – obrigatório;

**NOTA 9:** Imagem do documento de identificação em formato (JPG ou JPEG), com a face do

requerente disposta em pé, nomeado com o CPF do mesmo (exemplo: 11122233344.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB, em que se possa ler nitidamente todas as informações biográficas apresentadas no documento. Imagem da face em formato (JPG ou JPEG), com a face do requerente disposta em pé, nomeado com o CPF“FACE” do mesmo (exemplo: 11122233344FACE.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB (pode ser recortada do próprio documento de identificação).

xxv. Após todo o preenchimento dos campos do comunicado e *upload* das imagens, deve-se fazer uma verificação de todas as informações inseridas. Caso estejam corretas, deve ser enviado o comunicado ao ITI, conforme descrito no ADE-ICP-05.02.B [5] (Métodos de Interface do Serviço de Lista Negativa).

**NOTA 10:** Qualquer cancelamento de fraude, feito pelas AC por processos de auditoria e análise detalhada devem ser enviadas ao endereço de correio eletrônico: [comunicafraude@iti.gov.br](mailto:comunicafraude@iti.gov.br), com a descrição detalhada dos motivos do cancelamento.

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

3.3 Após o registro na lista negativa, encaminhar à DAFN o dossiê de emissão do certificado, os dossiês dos AGR que atuaram na identificação e cópia do Boletim de Ocorrência.



## 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.

<i>Ref.</i>	<i>Nome do documento</i>	<i>Código</i>
[1]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05
[2]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[3]	CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[4]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09

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

<i>Ref.</i>	<i>Nome do documento</i>	<i>Código</i>
[5]	MÉTODOS WEBSERVICE LISTA NEGATIVA E COMUNICADO DE FRAUDE	ADE-ICP-05.02.B
[6]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	DOC-ICP-05.03
[7]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01