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 1.0

23 de junho de 2015

Sumário

CONTROLE DE ALTERAÇÕES

Resolução que aprovou a alteração	Item alterado	Descrição da alteração
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.

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 apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil.
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;

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 sua DPC os procedimentos empregados pelas AR vinculadas a uma AC 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.

2.2.1. Documentos para efeitos de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original, 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) Caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;
e) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial; e
f) Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4.

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: Caso seja apresentada a Carteira Nacional de Habilitação – CNH, a AR deve proceder a verificação por meio de consulta à base de dados dos órgãos emissores da CNH.

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.

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;
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 10: 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 11: 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 400 KB, em 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 200 KB (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 12: 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.