

CASA CIVIL  
IMPrensa NACIONAL

PORTARIA IN/CC/PR Nº 21, DE 29 DE ABRIL DE 2026

O DIRETOR-GERAL DA IMPRENSA NACIONAL, no uso da competência que lhe foi subdelegada pelo art. 2º, § 3º da Portaria CC/PR nº 725, de 23 de julho de 2025, do Ministro de Estado da Casa Civil da Presidência da República, resolve:

Art. 1º Realocar os seguintes cargos em comissão e funções comissionadas no âmbito da Imprensa Nacional da Casa Civil da Presidência da República, constantes no Anexo III do Decreto nº 12.873, de 11 de março de 2026:

- I - Uma Função Comissionada de Assessor Técnico, código FCE 2.10, da Coordenação-Geral de Publicação, Produção e Preservação para a Imprensa Nacional;  
II - Um Cargo em Comissão de Assistente Técnico, código CCE 2.02, da Coordenação-Geral de Publicação, Produção e Preservação para a Imprensa Nacional;  
III - Um Cargo em Comissão de Assistente Técnico, código CCE 2.05, da Imprensa Nacional para a Divisão de Apoio;  
IV - Uma Função Comissionada de Assistente, código FCE 2.07, da Imprensa Nacional para a Coordenação de Governança;

V - Uma Função Comissionada de Assistente Técnico, código FCE 2.05, da Coordenação-Geral de Tecnologia da Informação para a Coordenação de Sistemas, Dados e Inovação;

VI - Uma Função Comissionada de Assistente, código FCE 2.07, da Coordenação-Geral de Administração para a Coordenação de Gestão de Pessoas;

VII - Um Cargo em Comissão de Assistente, código CCE 2.07, da Coordenação de Gestão de Pessoas para a Coordenação-Geral de Administração.

Art. 2º As realocações de que tratam o art. 1º serão refletidas no Quadro Demonstrativo dos Cargos em Comissão e das Funções Comissionadas da Imprensa Nacional da Casa Civil da Presidência da República e devem ser registradas no Sistema de Organização e Inovação Institucional do Governo Federal - SIOIG até o dia útil anterior à data de entrada em vigor desta Portaria.

Art. 3º Esta Portaria entra em vigor sete dias úteis após a data de publicação.

AFONSO OLIVEIRA DE ALMEIDA

## ANEXO

UNIDADE	SITUAÇÃO ATUAL			SITUAÇÃO NOVA		
	QUANTIDADE	DENOMINAÇÃO	CCE/FCE	QUANTIDADE	DENOMINAÇÃO	CCE/FCE
COORDENAÇÃO-GERAL DE PUBLICAÇÃO PRODUÇÃO E PRESERVAÇÃO DA IMPRENSA NACIONAL	01	ASSESSOR TÉCNICO	FCE 2.10	-	-	-
IMPrensa NACIONAL DA CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA	-	-	-	01	ASSESSOR TÉCNICO	FCE 2.10
COORDENAÇÃO-GERAL DE PUBLICAÇÃO PRODUÇÃO E PRESERVAÇÃO DA IMPRENSA NACIONAL	01	ASSISTENTE TÉCNICO	CCE 2.02	-	-	-
IMPrensa NACIONAL DA CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA	-	-	-	01	ASSISTENTE TÉCNICO	CCE 2.02
IMPrensa NACIONAL DA CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA	01	ASSISTENTE TÉCNICO	CCE 2.05	-	-	-
DIVISÃO DE APOIO DA IMPRENSA NACIONAL	-	-	-	01	ASSISTENTE TÉCNICO	CCE 2.05
IMPrensa NACIONAL DA CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA	01	ASSISTENTE	FCE 2.07	-	-	-
COORDENAÇÃO DE GOVERNANÇA DA IMPRENSA NACIONAL	-	-	-	01	ASSISTENTE	FCE 2.07
COORDENAÇÃO-GERAL DE TECNOLOGIA DA INFORMAÇÃO DA IMPRENSA NACIONAL	01	ASSISTENTE TÉCNICO	FCE 2.05	-	-	-
COORDENAÇÃO DE SISTEMAS, DADOS E INOVAÇÃO DA COORDENAÇÃO-GERAL DE TECNOLOGIA DA INFORMAÇÃO DA IMPRENSA NACIONAL	-	-	-	01	ASSISTENTE TÉCNICO	FCE 2.05
COORDENAÇÃO-GERAL DE ADMINISTRAÇÃO DA IMPRENSA NACIONAL	01	ASSISTENTE	FCE 2.07	-	-	-
COORDENAÇÃO DE GESTÃO DE PESSOAS DA COORDENAÇÃO-GERAL DE ADMINISTRAÇÃO	-	-	-	01	ASSISTENTE	FCE 2.07
COORDENAÇÃO DE GESTÃO DE PESSOAS DA COORDENAÇÃO-GERAL DE ADMINISTRAÇÃO	01	ASSISTENTE	CCE 2.07	-	-	-
COORDENAÇÃO-GERAL DE ADMINISTRAÇÃO DA IMPRENSA NACIONAL	-	-	-	01	ASSISTENTE	CCE 2.07

COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS  
BRASILEIRA - ICP-BRASIL

## INSTRUÇÃO NORMATIVA ITI Nº 36, DE 29 DE ABRIL DE 2026

Estabelece requisitos e procedimentos para a confirmação da identidade de requerente de certificado digital no âmbito da ICP-Brasil.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 13 do anexo I do Decreto nº 12.103, de 8 de julho de 2024, 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, resolve:

CAPÍTULO I  
DAS DISPOSIÇÕES GERAIS

Art. 1º Este Regulamento detalha os requisitos e procedimentos para a confirmação da identidade de requerente de certificado digital no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, visando aumentar a segurança, reduzir fraudes e simplificar o processo de emissão, complementando a Resolução CG ICP-Brasil nº 177, de 20 de outubro de 2020 (DOC-ICP-05).

§1º Os requisitos e procedimentos deste Regulamento não são exaustivos.

§2º As entidades da ICP-Brasil são responsáveis por garantir a segurança do processo de identificação do requerente, respondendo pelo dano que der causa.

§3º As Autoridades Certificadoras - ACs devem definir em suas Declarações de Práticas de Certificação - DPC os procedimentos empregados pelas suas Autoridades de Registro - ARs vinculadas para a confirmação da identidade de um indivíduo, observado o disposto neste Regulamento.

Art. 2º Os métodos admissíveis de confirmação de identidade são:

- I - comparecimento presencial;  
II - videoconferência;  
III - uso de certificado ICP-Brasil válido;  
IV - módulo Eletrônico de AR; e  
V - AR Eletrônica.

Parágrafo único. Os métodos admissíveis de confirmação de identidade diversos do comparecimento presencial devem assegurar nível de segurança equivalente à forma presencial, garantindo a validação das informações de identificação biográficas e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico.

Art. 3º A confirmação de identidade do requerente de certificado digital deve compreender, no mínimo:

- I - apresentação e verificação da documentação exigida;  
II - coleta e verificação biométrica;  
III - consulta à base de dados da Lista Negativa de ACs; e  
IV - assinatura ou confirmação da origem e integridade do Termo de Titoralidade, conforme o caso.

§1º É dispensada a validação dos documentos da pessoa física requerente, ou do responsável pelo certificado da pessoa jurídica, quando houver a identificação positiva de pelo menos uma impressão digital junto ao Sistema Biométrico da ICP-Brasil, exceto quando houver alteração de dados ou a necessidade de complementar a documentação.

§2º A coleta biométrica do requerente, a ser submetida à verificação, deve garantir que a biometria seja de uma pessoa viva presente no momento da prova de identidade, com uso de *liveness detection*, e que não haja sinais de fraude comportamental e simbólica, observando a Instrução Normativa ITI nº 09, de 22 de outubro de 2020, que aprova os Procedimentos para Identificação Biométrica na ICP-Brasil.

Art. 4º Os procedimentos de comprovação de identidade de que trata este Regulamento não se aplicam à 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.

Art. 5º As Bases Oficiais Nacionais admitidas na ICP-Brasil para fins de batimento biométrico e biográfico são as seguintes:

- I - base de dados da Carteira Nacional de Identidade - CIN;  
II - base de dados da Identificação Civil Nacional - ICN, mantida pelo Tribunal Superior Eleitoral - TSE;  
III - base de dados da Carteira Nacional de Habilitação, mantida pela Secretaria Nacional de Trânsito - Senatran; e  
IV - base de dados da Infraestrutura Pública Digital - IPD de Identificação Civil, prevista no Art. 18 do Decreto nº 12.069, de 21 de junho de 2024, mantida pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos.

Art. 6º Devem ser mantidos no dossiê do titular do certificado digital:

- I - os dados biográficos e biométricos do requerente;  
II - as cópias de todos os documentos apresentados;  
III - os resultados das consultas de verificação e validação dos documentos, dos dados biográficos e das biometrias;  
IV - as gravações, no caso da emissão por videoconferência;  
V - os Termos de Titularidade; e  
VI - as trilhas de auditoria.

Parágrafo único. 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.

CAPÍTULO II  
DOS MÉTODOS E PROCEDIMENTOS PARA CONFIRMAÇÃO DA IDENTIDADE

## Confirmação inicial da identidade

Art. 7º Os procedimentos e os requisitos para a primeira identificação e cadastramento junto à ICP-Brasil de pessoas físicas titulares ou responsáveis por certificados digitais devem compreender os seguintes processos:

I - identificação e cadastro iniciais do titular do certificado, com a identificação da pessoa física ou jurídica, titular do certificado, com base nos documentos de identificação citados neste Regulamento, observando ainda:

a) para certificado de pessoa física, a comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação e biometrias apresentadas, vedada qualquer espécie de procuração para tal fim; e

b) para certificado de pessoa jurídica, a comprovação de que os documentos apresentados se referem efetivamente à pessoa jurídica titular do certificado e de que a pessoa física que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição, admitida procuração por instrumento público, com poderes específicos para atuar perante a ICP-Brasil, cuja certidão original ou segunda via tenha sido emitida dentro de 90 (noventa) dias anteriores à data da solicitação.



II - emissão do certificado, pelo sistema da AC, após a conferência dos dados da solicitação de certificado com os constantes dos documentos e biometrias apresentados na etapa de identificação.

Parágrafo único. Todas as partes da extensão *Subject Alternative Name* 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.

#### Confirmação da identidade de um indivíduo

Art. 8º Para a identificação da pessoa física requerente do certificado, é necessário:

- I - apresentar a seguinte documentação, em sua versão original oficial:
- Carteira de Identidade Nacional - CIN ou outro Registro de Identidade, se brasileiro; ou
  - Carteira Nacional de Estrangeiro - CNE, se estrangeiro domiciliado no Brasil; ou
  - Passaporte, se estrangeiro não domiciliado no Brasil;
- II - consultar a inscrição no Cadastro de Pessoa Física - CPF;
- III - verificar o eventual enquadramento do requerente como Pessoa Exposta Politicamente - PEP, autoridade do Poder Judiciário ou do Ministério Público, de acordo com a legislação vigente; e
- IV - coletar e verificar a biometria do requerente, considerando:
- impressão digital e face, se em emissão presencial; e
  - no mínimo, biometria facial, se emissão por videoconferência, Módulo Eletrônico de AR ou AR Eletrônica.

§1º Para fins desta Instrução Normativa, somente serão admitidos como registro de identidade mencionado na alínea "a", do inciso I, do caput, documentos oficiais emitidos por autoridade legalmente competente, nos termos da legislação, bem como aqueles equiparados por lei a documento de identidade válido em todo o território nacional, desde que contenham fotografia.

§2º É vedada a utilização de documento de registro de identidade que impossibilite a realização de batimento biométrico facial.

§3º Sempre que o documento de identificação apresentado não possibilitar a identificação inequívoca, inclusive por deterioração, desatualização ou alteração física do requerente, a AR deve exigir documento adicional.

§4º A emissão do certificado deve ser negada, caso persista a impossibilidade de identificação inequívoca mencionada no §3º.

§5º Todos os documentos utilizados no processo de confirmação da identidade devem ser validados nas bases de dados e aplicativos oficiais.

§6º Para os documentos mencionados no §5º que contenham tecnologias verificáveis, como QR Code, MRZ, NFC, Chip ou similares, a validação do código ou tecnologia embarcada deverá ser realizada, sendo vedada a emissão caso a validação apresente inconsistências.

§7º É vedada a emissão de certificados para pessoas físicas com situação cadastral "cancelada", "nula" ou "falecida" junto à Receita Federal do Brasil.

Art. 9º Deve ser realizada etapa de verificação por Agente de Registro - AGR distinto do que realizou a etapa de identificação, vinculado à AR, à AR própria da AC ou à AR própria do PSS da AC, nas seguintes situações:

- para documentos impressos para os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais;
- para requerentes não cadastrados no Prestador de Serviço Biométrico - PSBio, exceto para emissão por AR Eletrônica ou Módulo Eletrônico de AR; e
- para Pessoas Expostas Politicamente - PEP.

Parágrafo único. A verificação de que trata o caput deverá ser realizada antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

Art. 10. A verificação biométrica do requerente deverá ser realizada por meio de batimento dos dados nas Bases Oficiais Nacionais previstas neste Regulamento, observando a Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

#### Confirmação da Identidade de Organizações

Art. 11. Será designado como responsável pelo certificado o representante legal da pessoa jurídica requerente do certificado, ou o procurador constituído na forma do art. 7º, inciso I, alínea 'b', deste Regulamento, o qual será o detentor da chave privada.

Art. 12. Deve ser realizada a confirmação da identidade da organização e da pessoa física responsável pelo certificado, bem como a verificação da origem e integridade do Termo de Titularidade, conforme disposto neste Regulamento.

Art. 13. A apresentação dos documentos da pessoa física responsável, bem como a coleta e verificação dos seus dados biométricos, são dispensáveis 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.

Parágrafo único. O disposto neste artigo não afasta a necessidade de apresentação dos documentos pertinentes à pessoa jurídica requerente, ou os demais requisitos exigidos para identificação do requerente.

Art. 14. A confirmação da identidade de uma pessoa jurídica deve ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

- relativos à sua habilitação jurídica:
  - se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do CNPJ;
  - se entidade privada:
    - certidão simplificada emitida pela Junta Comercial ou ato constitutivo, devidamente registrado no órgão competente, que permita a comprovação de quem são seus atuais representantes legais; e
    - documentos da eleição de seus representantes legais, quando aplicável;
- relativos à sua habilitação fiscal:
  - prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ; ou
  - prova de inscrição no Cadastro Nacional de Obras - CNO.

§1º As confirmações de que tratam o caput deste artigo podem ser feitas de forma eletrônica, desde que em barramentos ou aplicações oficiais.

§2º É obrigatório que as validações mencionadas no §1º constem no dossiê eletrônico do titular do certificado.

§3º É vedada a emissão de certificados para pessoas jurídicas com situação cadastral "Baixada" ou "Nula" junto à Receita Federal do Brasil.

#### Identificação de equipamentos ou aplicações

Art. 15. Em se tratando de certificado emitido para equipamento ou aplicação, o titular é a pessoa física ou jurídica solicitante do certificado, que deve confirmar sua identidade nos termos deste Regulamento e indicar o responsável pela chave privada.

Art. 16. Para certificados de aplicações específicas que utilizem URL na identificação do titular deve ser verificado se o solicitante do certificado detém o registro do nome de domínio junto ao órgão competente, ou se possui autorização do titular do domínio para utilizá-lo.

Parágrafo único. Nos casos estabelecidos no caput, deve ser apresentada a documentação comprobatória (termo de autorização de uso de domínio ou similar).

Art. 17. Para a emissão de certificados do tipo T3 ou T4, para equipamentos de Autoridades de Carimbo do Tempo - ACT credenciadas na ICP-Brasil, a solicitação deve conter o nome de servidor e o número de série do equipamento.

Parágrafo único. Os dados referentes à emissão mencionada no caput devem ser validados comparando-os com aqueles publicados pelo ITI no Diário Oficial da União, quando do deferimento do credenciamento da ACT.

#### Identificação de equipamento para certificado CF-e-SAT

Art. 18. A validação de solicitação de certificado do tipo A CF-e-SAT compreende:

- validar o registro inicial por meio de verificação da origem e integridade da solicitação do certificado A CF-e-SAT e do Termo de Titularidade específico;
- realizar a verificação da solicitação contendo a requisição em conformidade com o formato estabelecido na Instrução Normativa ITI nº 22, de 23 de março de 2022, que aprova os Padrões e Algoritmos Criptográficos da ICP-Brasil, e confrontando com as informações (número de segurança e número de série do equipamento SAT e CNPJ do contribuinte emissor CF-e) do registro inicial e do certificado digital utilizado na solicitação;

III - emissão do certificado digital sem que haja possibilidade de alteração dos dados constantes na requisição e disponibilização ao solicitante para instalação no equipamento SAT.

Parágrafo único. O certificado digital do contribuinte que garante a origem e integridade da solicitação e do Termo de Titularidade referido no inciso I do caput deve ser um certificado digital de selo eletrônico ICP-Brasil válido.

Art. 19. Em se tratando de certificado emitido para equipamento SAT, o titular será representado pelo representante legal da pessoa jurídica requerente, associado ao número de série do equipamento detentor da chave privada.

Art. 20. Para certificados de equipamento SAT, deve ser verificado se o CNPJ do contribuinte que solicita esse certificado está vinculado ao número de série do referido equipamento, o qual deve estar registrado e autorizado pela unidade fiscal federada.

Parágrafo único. As informações mencionadas no caput devem ser obtidas e confirmadas pela AC emissora do certificado.

#### Identificação de equipamento para certificado OM-BR

Art. 21. A validação de solicitação de certificado do tipo OM-BR compreende:

- validar o registro inicial por meio de verificação da origem e integridade da solicitação do certificado OM-BR e do Termo de Titularidade específico;
- realizar a verificação da solicitação contendo a requisição em conformidade com o formato estabelecido na Instrução Normativa ITI nº 22, de 23 de março de 2022, que aprova os Padrões e Algoritmos Criptográficos da ICP-Brasil, e confrontando com as informações de controle do órgão regulador e do certificado digital utilizado na solicitação;
- emissão do certificado digital sem que haja possibilidade de alteração dos dados constantes na requisição e disponibilização ao solicitante para instalação no equipamento OM-BR.

Parágrafo único. O certificado digital do fabricante que garante a origem e integridade da solicitação e do Termo de Titularidade referidos no inciso I do caput deve ser um certificado digital de selo eletrônico ICP-Brasil válido.

Art. 22. Em se tratando de certificado emitido para equipamento OM-BR, o titular será representado pelo fabricante identificado no certificado de selo digital que o solicita, associado ao número de identificação do equipamento detentor da chave privada.

Art. 23. Para certificados do tipo OM-BR, deve ser verificado se o CNPJ do fabricante que solicita esse certificado está vinculado aos controles regulatórios do referido equipamento, o qual deve estar registrado e autorizado pelo Inmetro.

Parágrafo único. As informações mencionadas no caput devem ser obtidas e confirmadas pela AC emissora do certificado.

#### Procedimentos para confirmação de identidade

Art. 24. 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 regras dispostas no documento ADE-ICP-05.02.B (Métodos de Interface do Serviço de Lista Negativa), durante o processo de identificação de requerente de um certificado digital ICP-Brasil.

§1º A base de dados da Lista Negativa da AC, mencionada no caput deste artigo, deve ser atualizada pela comunicação entre o PSBio, servidor da AC e o servidor do ITI, conforme disposto no ADE-ICP-05.02.B.

§2º Ao consultar a Lista Negativa, com o objetivo de identificar possíveis fraudadores, o AGR deverá confrontar:

- as informações biográficas dos documentos de identificação apresentados, ou as informações dos documentos de constituição da pessoa jurídica, quando for o caso, com aquelas que constam registradas em tal Lista Negativa; e
- o resultado do confronto biométrico do requerente com as biometrias constantes da Lista Negativa (1:N), conforme disposições sobre a base de fraudadores da Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

§3º Após a realização da consulta à Lista Negativa da AC, as seguintes providências devem ser adotadas:

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

Art. 25. 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.

§1º A interface da aplicação para os AGRs, mencionada no caput deste artigo, deve possibilitar consulta pelo CPF (indexador) do requerente do certificado digital, com a coleta das biometrias do requerente, as quais devem ser comparadas obrigatoriamente com o registro daquelas biometrias específicas no Sistema de Dados Biométricos da ICP-Brasil ou em Bases Oficiais Nacionais.

§2º Na emissão presencial do certificado digital, a Autoridade de Registro deve observar os seguintes procedimentos de verificação e atualização biométrica:

- para titulares com impressão digital previamente cadastrada, é obrigatória a realização da verificação (*match*) da impressão digital, devendo o resultado ser registrado no dossiê de atendimento; e
- para titulares que possuam apenas biometria facial registrada, a AR deve coletar as impressões digitais do titular, com a finalidade de complementar e atualizar o respectivo cadastro biométrico no âmbito da ICP-Brasil, de acordo com os procedimentos definidos na Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

§3º Deverá ser realizada nova captura biométrica facial e atualização cadastral, conforme procedimentos definidos na Instrução Normativa ITI nº 09, de 22 de outubro de 2020, se a biometria existente no PSBio tiver mais de cinco anos, aplicável a validações presenciais e por videoconferência.

Art. 26. Nos procedimentos de coleta, verificação e identificação biométrica do requerente junto ao Sistema Biométrico da ICP-Brasil e às Bases Oficiais Nacionais para emissão de certificado digital ICP-Brasil é necessário observar o seguinte:

- o Sistema Biométrico da ICP-Brasil deve informar ao AGR qual é o "melhor dedo", no caso de verificação da biometria da impressão digital;
- caso nenhuma impressão digital tenha qualidade para verificação da biometria, o requerente não poderá ser identificado pelo processo da verificação biométrica da impressão digital;
- quando não houver possibilidade de utilização da impressão digital, conforme indicado na Instrução Normativa ITI nº 09, de 22 de outubro de 2020, nas disposições que tratam dos parâmetros mínimos para coleta da impressão digital, deve ser utilizada a biometria da face;
- 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 na Instrução Normativa ITI nº 09, de 22 de outubro de 2020, bem como adotar as demais providências para confirmação da identidade;
- caso o CPF (indexador) esteja na base de dados biométrica 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 erro), considerando que:
  - o resultado "positivo" da consulta à base de dados biométrica significa que foi obtido o atingimento pleno da taxa de aceitação da acurácia estabelecida na Instrução Normativa ITI nº 09, de 22 de outubro de 2020; e



b) o resultado "negativo" da consulta à base de dados biométrica significa que não se obteve o atingimento da taxa de aceitação da acurácia estabelecida na Instrução Normativa ITI nº 09, de 22 de outubro de 2020;

VI - o resultado "positivo" da consulta à base de dados biométrica da ICP-Brasil ou a Bases Oficiais Nacionais deve ser apensado ao dossiê do titular do certificado e preservados de acordo com a Instrução Normativa ITI nº 10, de 22 de outubro de 2020;

VII - caso o resultado da verificação biométrica no Sistema Biométrico da ICP-Brasil tenha encontrado o CPF (indexador - Identificador de registro biométrico - IDN) do requerente com o resultado da comparação "negativo", deve-se comunicar à AC vinculada para que se faça uma análise detalhada do caso, observando-se:

a) se a AC concluir que o requerente se trata do titular de fato do documento de identificação e/ou das informações da empresa, deve dar prosseguimento ao processo de emissão do certificado digital, com a análise dos demais requisitos exigidos;

b) na hipótese de o 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, a AC deve realizar os procedimentos de notificação de irregularidades mencionados na Instrução Normativa ITI nº 09, de 22 de outubro de 2020;

c) caso a AC concluir que se trata de tentativa de fraude, não deve emitir o certificado digital e deve comunicar ao ITI, conforme Capítulo VI deste Regulamento;

VIII - todos os logs de transação biométrica feitos pelo AGR devem ser guardados pelo período mínimo de 7 (sete) anos pelas ACs.

Art. 27. Os dados cadastrais e biométricos do requerente devem ser validados junto à base da Carteira Nacional de Habilitação - CNH via Datavalid em todas as emissões.

Parágrafo único. Ficam dispensadas desse procedimento as ACs públicas (órgãos e entidades da Administração Direta da União, dos Estados, do Distrito Federal e dos Municípios, bem como suas autarquias e fundações públicas) em emissões presenciais com batimento da impressão digital, exclusivamente para o público interno.

Art. 28. Deve ser realizada a verificação de posse de e-mail, considerando que:

I - o mesmo endereço de e-mail não poderá ser vinculado a mais de um CPF;

II - a comprovação da posse do e-mail deverá ser realizada por meio de envio de código OTP (One-Time Password), que deverá ser informado pelo requerente durante o atendimento; e

III - o sistema da AC deverá validar o código OTP em tempo real e registrar o resultado da verificação no dossiê eletrônico do titular.

Art. 29. A emissão do certificado, ou seu início de validade, está condicionada à validação dos dados biométricos na base do PSBio ou em seu cache, sendo vedada a emissão do certificado digital com verificação biométrica realizada exclusivamente na base local da Autoridade Certificadora.

Parágrafo único. A AC deve solicitar a exclusão do cadastro no PSBio quando as etapas de identificação, validação e verificação de titularidade não forem concluídas.

Art. 30. Todo o processo de identificação do titular do certificado deve ser registrado com verificação biométrica e assinado digitalmente pelos executantes, na solução de certificação disponibilizada pela AC, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3.

§1º O sistema biométrico da ICP-BRASIL deve solicitar aleatoriamente qual dedo o AGR deve apresentar para autenticação, o que exige a inclusão de todos os dedos dos AGRs no cadastro do sistema biométrico.

§2º Os registros do processo de identificação mencionados no caput devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

#### Procedimentos específicos de identificação

Art. 31. Para requerentes identificados como Pessoas Expostas Politicamente - PEP ou autoridades do Poder Judiciário e do Ministério Público, será obrigatório:

I - segunda verificação por Agente de Registro da AC;

II - batimento da impressão digital na base do PSBio;

III - coleta de documento de identidade mesmo com batimento no PSBio; e

IV - adoção de procedimentos de segurança adicionais.

Art. 32. A emissão de certificados para incapazes, relativamente incapazes, tutelados ou curatelados, além de observar o disposto na lei vigente, exigirá:

I - identificação e coleta biométrica obrigatória do representante e do representado, salvo impossibilidade justificada, no caso do representado;

II - apresentação e validação dos documentos comprobatórios da condição específica (certidão, termo de tutela, sentença de curatela etc.); e

III - registro completo das validações e evidências no dossiê eletrônico.

Art. 33. A emissão de certificado digital de pessoa jurídica destinado a condomínios obedecerá ao disposto sobre identificação de organizações.

§1º Quando não for possível a identificação na forma mencionada no caput, deverão ser apresentados:

I - ato de constituição do condomínio; e

II - ata da Assembleia Condominial que elegeu o síndico ou administrador.

§2º Entende-se como ato constitutivo do condomínio o testamento, a escritura pública ou particular de instituição, ou a convenção condominial devidamente registrada no Cartório de Registro de Imóveis, não bastando, para tal fim, quaisquer outros documentos, tais como o regimento interno ou declarações emitidas pelos respectivos síndicos ou administradores.

§3º Para os condomínios devidamente inscritos perante o CNPJ, mas que não se encontrem regularmente constituídos nos termos da legislação vigente, fica dispensado o registro de seus atos constitutivos junto ao Cartório de Registro de Imóveis, a que se refere o §2º.

§4º As ARs e ACs poderão exigir outros documentos que considerem necessários para fins de comprovação da existência ou da representatividade do condomínio.

#### Identificação e autenticação para pedidos de novas chaves

Art. 34. A identificação e autenticação para os pedidos de novas chaves podem ser conduzidos por:

I - adoção dos mesmos requisitos e procedimentos exigidos nos dispositivos referentes à confirmação da identidade de um indivíduo, à confirmação da identidade de organizações e à identificação de equipamentos ou aplicações, todos constantes deste Regulamento;

II - solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICP-Brasil válido, do tipo A3 ou superior, cujo certificado requisitado seja do mesmo nível de segurança ou inferior; ou

III - videoconferência.

Art. 35. Para certificados de aplicações específicas que utilizem URL, a AC poderá implementar mecanismos automatizados de gerenciamento de certificado (ACME) de forma a preservar a posse ou propriedade da URL (domínio) e a identificação do solicitante, seja pessoa física ou jurídica.

Parágrafo único. O processo automatizado mencionado no caput implica as seguintes etapas:

I - o solicitante submete uma requisição de certificado (PKCS#10) da URL desejada;

II - a requisição deverá ser acompanhada do certificado da URL solicitada, ainda válido, e o conjunto (requisição + certificado da URL) deve ter a origem e integridade garantida por certificado ICP-Brasil;

III - o aplicativo de AR valida a origem e integridade da solicitação e a requisição e, caso esteja em conformidade, encaminha desafio de prova de domínio e o Termo de Titularidade;

IV - o solicitante responde o desafio e aceita o Termo de Titularidade com o mesmo certificado utilizado, mencionado no inciso II deste parágrafo único;

V - confirmado atendimento pleno do desafio e da origem e integridade do Termo de Titularidade, o aplicativo de AR poderá emitir o certificado e encaminhá-lo ao solicitante; e

VI - todas as evidências do processo acima devem constar no dossiê do certificado.

#### CAPÍTULO III DA IDENTIFICAÇÃO POR VIDEOCONFERÊNCIA

Art. 36. A identificação de requerente de certificado digital por videoconferência deve ser realizada por meio de comunicação interativa que permita a transmissão e captação de som, imagem e dados.

Art. 37. A videoconferência deve ser realizada obrigatoriamente por meio de solução tecnológica da Autoridade Certificadora, dotada de mecanismos de segurança que garantam a autenticidade, a integridade e a confidencialidade das informações capturadas.

§1º A solução tecnológica mencionada no caput deve assegurar que os meios técnicos utilizados são adequados para garantir que a videoconferência:

I - permita a detecção obrigatória de vivacidade (*liveness*) do requerente para minimizar o risco de manipulação de rosto e voz em montagens de vídeo conhecidas como "deepfake", com emprego de meios de detecção de ataque de apresentação para garantir que a biometria utilizada para a identificação seja de uma pessoa viva presente no momento da prova de identidade e que não se trata de um fraudador;

II - aplique meios de prevenção e detecção de ataques de injeção biométrica para assegurar que nem o requerente nem um atacante externo possam injetar, de forma indetectável, um fluxo de vídeo previamente gravado ou artificialmente gerado;

III - permita a detecção e bloqueio de drivers de câmeras virtuais, a detecção de integridade e o bloqueio de dispositivos comprometidos;

IV - permita que o AGR aplique questionários sequenciais (*scripts*) obrigatórios, de forma aleatória, de modo que a sequência de perguntas nunca seja a mesma e, portanto, não possa ser prevista;

V - seja realizada em tempo real e sem interrupções ou pausas;

VI - tenha qualidade adequada de som e imagem para permitir a identificação clara do requerente, das validações dos documentos de identificação, das verificações de face nas bases biométricas e biográficas e a verificação posterior dos dados de identificação recolhidos e comprovados;

VII - seja gravada com indicação da respectiva data e hora sincronizada com a Fonte Confiável do Tempo - FCT da ICP-Brasil;

VIII - tenha duração suficiente para assegurar a integral observância dos procedimentos completos de identificação do requerente; e

IX - preserve a integridade e a confidencialidade da comunicação audiovisual entre o AGR e o requerente por meio da utilização de sessões de vídeo protegidas com criptografia "ponta-a-ponta".

§2º A solução tecnológica mencionada no caput deverá ser testada periodicamente por entidades independentes, de modo a avaliar o desempenho e efetividade das tecnologias de detecção de ataque de apresentação.

§3º Na impossibilidade de realização de detecção de vivacidade, conforme disposto no inciso I, do §1º, por parte do requerente, este deve ser direcionado para outra modalidade de emissão de certificado, por meio da qual seja possível a coleta da biometria da impressão digital.

§4º Os questionários mencionados no inciso IV, do §1º, devem ser entendidos como um conjunto de perguntas feitas ao requerente, que permitam ao AGR coletar informações que atestem a veracidade da identificação da pessoa que se apresenta em vídeo.

Art. 38. No processo de identificação do requerente, devem ser observados os seguintes procedimentos:

I - antes da videoconferência, o requerente deverá enviar fotografia do documento de identificação físico e fotografia da face por meio da aplicação da AC, de forma a permitir a realização de batimentos prévios;

II - ao iniciar a videoconferência, o requerente deve dar autorização expressa a todo o processo de identificação, incluindo a captura de fotografias, imagens, voz, documentos de identificação, a submissão de verificação ao Sistema Biométrico ICP-Brasil e nas Bases Oficiais Nacionais, a gravação da videoconferência e a inclusão de todas as informações, gravações e arquivos em dossiê eletrônico do titular do certificado;

III - durante a videoconferência, o requerente deverá informar o número do seu CPF e apresentar a versão física do documento enviado previamente, que deve ser analisado e validado antes da emissão do certificado digital;

IV - a AR deve avaliar os dados dos documentos de identificação apresentados e realizar a confirmação da identidade do requerente, comunicando eventuais irregularidades, conforme disposto no Capítulo VI deste Regulamento;

V - havendo problema na validação dos documentos de identificação fornecidos pelo requerente, este deverá ser informado do problema ocorrido para que busque solucioná-lo, sob pena de não ter o certificado digital emitido; e

VI - durante a videoconferência, deve ser capturada a imagem da face (*frame*) do titular requerente, se pessoa física, ou do responsável pelo certificado, se pessoa jurídica, com indicação da data e hora da captura, observados os procedimentos de coleta e identificação biométrica na ICP-Brasil definidos na Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

§1º Para os documentos mencionados no inciso III, do caput, que contenham tecnologias verificáveis, como QR Code, MRZ (Machine Readable Zone), NFC, Chip ou similares, a validação do código ou tecnologia embarcada deverá ser realizada durante a videoconferência, por meio de leitura automatizada ou verificação manual assistida.

§2º Feita a coleta da biometria facial (*frame*), nos termos do inciso VI, do caput, deverá ser realizada verificação biométrica de face (1:1) com as fotografias do documento de identificação e da face previamente encaminhadas, conforme estabelecido no inciso I, do caput deste artigo.

§3º A verificação biométrica de que trata o §2º deverá ser realizada por meio de *software* a ser disponibilizado pela AC à AR, observando-se o seguinte:

I - caso o resultado dessa verificação biométrica seja "negativo", deve-se interromper o processo e comunicar à AC vinculada para que seja feita uma análise detalhada do caso;

II - concluindo a AR ou a AC que o requerente se trata, de fato, do titular do documento de identificação, deverá ser dado prosseguimento ao processo de identificação; ou

III - concluindo a AR ou a AC se tratar de tentativa de fraude, não deverá ser emitido o certificado digital e a AC deve realizar o procedimento de comunicação de fraude ao ITI.

Art. 39. Além da verificação biométrica junto ao documento de identificação, o AGR deve confirmar a identidade do requerente em procedimento de verificação biométrica (1:1) junto ao Sistema Biométrico ICP-Brasil ou, se acaso não constar desta, a verificação biométrica (1:1) e biográfica do requerente será submetida às Bases Oficiais Nacionais admitidas na ICP-Brasil.

§1º Caso o requerente já possua cadastro biométrico na ICP-Brasil, a verificação biométrica (1:1) deve ser realizada junto ao Sistema Biométrico ICP-Brasil, observando-se os procedimentos gerais para confirmação de identidade constantes neste Regulamento, sobretudo o inciso VII, do caput, do art. 26.

§2º Na hipótese de o requerente não possuir cadastro no Sistema Biométrico ICP-Brasil, a verificação biométrica (1:1) e biográfica deste será submetida às Bases Oficiais Nacionais admitidas na ICP-Brasil.

§3º A verificação biométrica e biográfica realizada durante o processo de videoconferência deverá observar critérios mínimos de aceitação e implementar travas sistêmicas, com base nos scores de probabilidade retornados pelas Bases Oficiais Nacionais ou serviços integrados, como o Datavalid, que considera que:

I - o processo para emissão do certificado deve prosseguir, em caso de probabilidade altíssima;

II - uma análise complementar por segundo agente especializado deve ser requerida, em caso de probabilidade alta; ou

III - o processo deve ser redirecionado para emissão presencial, em caso de probabilidade média.

§4º Caso o requerente não esteja cadastrado em Base Oficial Nacional, o processo de identificação por videoconferência deverá ser interrompido pelo AGR, encaminhando-se o requerente para o processo de emissão presencial.

§5º Concluindo a AR e a AC se tratar de tentativa de fraude, não deverá ser emitido o certificado digital e a AC deve realizar o procedimento de comunicação de fraude ao ITI, descrito neste Regulamento.



Art. 40. No caso de certificado de pessoa jurídica, a identificação do responsável pelo certificado obriga a confirmação da identificação da pessoa jurídica requerente, obrigatoriamente em formato eletrônico, verificável por meio de barramento ou aplicações oficiais, conforme disposto neste Regulamento.

Parágrafo único. O AGR deve certificar-se de que as informações da pessoa jurídica constantes no documento de identificação apresentado correspondem efetivamente à pessoa jurídica requerente a ser identificada, bem como sobre a veracidade da informação contida no documento de identificação do requerente, quando um documento de identificação for utilizado.

Art. 41. Caso não se verifiquem as condições técnicas necessárias à boa condução do processo de identificação e cadastro ou de comprovação da identidade, nomeadamente nos casos de existência de fraca qualidade de imagem, de condições deficientes de luminosidade ou som, ou de interrupções na transmissão do vídeo, a videoconferência deverá ser interrompida e considerada sem efeito.

Art. 42. Durante a realização da videoconferência, deve ser enviado ao requerente um código de verificação, único e descartável, do tipo OTP, por canal distinto da videoconferência, que assegure a integral rastreabilidade do procedimento de identificação e a realização da videoconferência em tempo real e sem pausas, gerado centralmente e enviado para o requerente por e-mail, SMS ou aplicativo móvel.

Parágrafo único. O procedimento de identificação só se considera completo após o requerente informar o código de verificação, mencionado no caput, e realizada a confirmação desse código único pelo sistema.

Art. 43. Sempre que, durante a videoconferência, existam suspeitas quanto à veracidade dos elementos de identificação, a videoconferência não produz os efeitos de comprovação dos elementos identificativos a que se destina.

Art. 44. As ACs devem estabelecer e garantir que suas ARs cumpram controles adicionais para mitigação de riscos no processo de emissão por videoconferência, compatíveis com o nível de risco identificado, destinados a assegurar a integridade, a autenticidade e a confiabilidade do processo de identificação.

Parágrafo único. Em casos de alto risco, deverá ser realizada a etapa de verificação prevista no art. 9º deste Regulamento.

Art. 45. O Agente de Registro deve receber treinamento específico e periódico que os capacite a realizar identificação remota assistida, a aplicar os mecanismos de detecção de ataque de apresentação e a identificar indícios de manipulação de mídia e imagem.

Parágrafo único. O Agente de Registro deverá ser avaliado quanto à sua capacidade de realizar a identificação remota assistida.

#### CAPÍTULO IV DO MÓDULO ELETRÔNICO DE AR

Art. 46. O Módulo Eletrônico de AR pode ser utilizado por:

- I - AR dos órgãos gestores de pessoas, na emissão de certificados para:
  - a) servidores públicos federais da ativa e militares da União;
  - b) servidores públicos estaduais e do Distrito Federal da ativa, desde que as Unidades da Federação possuam um Sistema de Gestão de Pessoal com individualização inequívoca e eletrônica, e que identifiquem biometricamente os servidores pela base do TSE, PSBios ou base oficial equivalente, com comprovação auditável desses cadastros; e
  - c) Empregados públicos federais de empresas estatais dependentes do orçamento público federal para custeio de pessoal, desde que vinculados ao Sistema de Gestão de Pessoal da Administração Pública Federal - SIGEP;
- II - AR de Bancos Múltiplos ou Caixa Econômica Federal;
- III - as serventias extrajudiciais vinculadas a uma AR;
- IV - ARs dos conselhos de classes profissionais regulamentados por lei específica e em conformidade com a Lei nº 6.206, de 07 de maio de 1975;
- V - ARs com acesso eletrônico às bases de dados das juntas comerciais, para solicitação de certificado por meio do Balcão Único para Abertura de Empresas; e
- VI - Órgão de Identificação ou Departamento de Trânsito - Detran dos Estados e do Distrito Federal, para emissão conjunta com a Carteira de Identidade Nacional - CIN ou a Carteira Nacional de Habilitação - CNH.

Art. 47. São requisitos e procedimentos comuns do Módulo Eletrônico de AR:

- I - ser um sistema vinculado a uma AC credenciada pela ICP-Brasil;
- II - possuir, de forma segura, registros de trilhas de auditoria;
- III - ser auditado pelo ITI em procedimento pré-operacional;
- IV - comunicar-se diretamente, utilizando protocolos de comunicação seguros, com os sistemas determinados formalmente pelas entidades autorizadas a utilizar Módulo Eletrônico de AR;
- V - obter os dados para gerar a requisição do certificado à AC diretamente de seus respectivos sistemas eletrônicos ou base de dados, sem que haja qualquer possibilidade de alteração desses;
- VI - ter a requisição do certificado assinada por funcionário autorizado como Agente de Registro devidamente cadastrado no sistema da AC, sendo a AC responsável por manter as respectivas requisições para fins de auditoria e fiscalização pela AC Raiz;
- VII - o requerente deverá ter sido biometricamente identificado e individualizado pela respectiva base biométrica ou PSBio da ICP Brasil, com comprovação auditável do cadastro desses requerentes por parte da AC;
- VIII - as biometrias e dados biográficos utilizados deverão ser compartilhadas com a AC, que deverá submetê-las ao PSBio para cadastramento e batimento biométrico (1:N), ou, caso o responsável já se encontre cadastrado, para o batimento biométrico (1:1) junto à ICP-Brasil;
- IX - em qualquer hipótese, deve ser realizada a consulta à Lista Negativa do PSBio, devendo proceder conforme regulamentado para as situações em que haja conflito de identificação biométrica detectada pelo PSBio ou ocorrência de registro na Lista Negativa; e
- X - possuir listas atualizadas com os nomes e CPF dos funcionários autorizados como Agentes de Registro a verificar as informações de solicitações de certificados por titulares.

§1º Os autorizadores, conforme mencionado no inciso X do caput, serão formalmente designados por instrumento próprio.

§2º No caso de impossibilidade da autenticação biométrica por qualquer das formas previstas, deverá ser realizada a identificação biométrica do responsável por meio do cadastramento biométrico (1:N) junto ao PSBio credenciado, conforme as normas vigentes da ICP-Brasil.

Art. 48. Para as ARs que utilizam exclusivamente Módulo Eletrônico de AR nas emissões de certificados, ficam dispensados os requisitos dispostos na Instrução Normativa ITI nº 10, de 22 de outubro de 2020, que define as características mínimas de segurança para as ARs da ICP-Brasil.

#### Procedimentos Específicos

Art. 49. Caso a solicitação de certificado seja realizada por meio do Balcão Único para Abertura de Empresas, as ARs com acesso eletrônico às bases de dados das juntas comerciais deverão observar o seguinte:

I - o responsável pelo uso do certificado de selo eletrônico deverá ser autenticado por meio de certificado digital de pessoa física ICP-Brasil válido ou por meio de batimento biométrico (1:1) em PSBio credenciado na ICP-Brasil, na base biométrica oficial do TSE ou em outra base biométrica oficial da União, dos Estados ou do Distrito Federal, com comprovação auditável desse processo de autenticação biométrica por parte da AC; e

II - o indivíduo identificado ou autenticado pelo Módulo Eletrônico de AR deverá ser representante legal da pessoa jurídica titular do certificado, conforme conste no registro de abertura de empresa concomitante com a solicitação do respectivo certificado.

Parágrafo único. A comprovação auditável mencionada no inciso I, do caput, poderá ser realizada pelo CPF ou outro indexador viável entre os sistemas.

Art. 50. Caso a solicitação de certificado a ser emitido em conjunto com a Carteira de Identidade Nacional - CIN ou a Carteira Nacional de Habilitação - CNH, deverão ser observados os seguintes requisitos:

I - a pessoa física titular do certificado deverá ter sido biometricamente identificada e individualizada na base biométrica do órgão responsável pela emissão da Carteira de Identidade Nacional - CIN ou da Carteira Nacional de Habilitação - CNH, conforme o caso, bem como ter dado consentimento expresso e específico para o compartilhamento com as entidades da ICP-Brasil dos dados biométricos e biográficos necessários para a identificação, cadastro e emissão do certificado digital; e

II - a AC contratada somente poderá emitir o certificado digital na modalidade em Prestador de Serviço de Confiança - PSC de armazenamento de chaves criptográficas e a habilitação do uso de chaves somente poderá ocorrer após o batimento biométrico (1:1) ou após conclusão do cadastramento biométrico.

Parágrafo único. A individualização na base biométrica, mencionada no inciso I, do caput, poderá ser realizada pelo CPF ou outro indexador viável entre os sistemas.

#### CAPÍTULO V DA AR ELETRÔNICA

Art. 51. A emissão por AR Eletrônica é restrita a certificado de pessoa física e deve utilizar canal eletrônico automatizado e sem intervenção humana, baseando-se na validação biométrica em bases reconhecidas pela ICP-Brasil.

Art. 52. A emissão de certificado na modalidade AR Eletrônica é restrita à Autoridade Certificadora com instalações operacionais, recursos de segurança lógica e de pessoas compatíveis com a atividade de certificação.

Art. 53. A emissão por AR Eletrônica deve ser realizada exclusivamente por meio de dispositivo móvel, com aplicativo (APP) guiado da AC dotado de mecanismos de segurança que garantam, autenticidade, integridade e confidencialidade das informações capturadas.

Art. 54. O início da operação na modalidade AR Eletrônica está condicionado à autorização pelo ITI, que verificará a disponibilização do aplicativo da AC nas respectivas plataformas de distribuição dos provedores de sistemas operacionais de dispositivos móveis.

Art. 55. A chave privada do certificado digital emitido por meio de AR Eletrônica deverá ser gerada e mantida por Prestador de Serviço de Confiança - PSC.

Art. 56. É vedada a emissão de certificado na modalidade de AR Eletrônica para Pessoas Expostas Politicamente - PEP ou autoridades do Poder Judiciário e do Ministério Público.

#### Requisitos e procedimentos para emissão por AR Eletrônica

Art. 57. O aplicativo guiado da AC deve:

I - preservar a integridade e a confidencialidade da comunicação entre o APP e sistemas da AC por meio da utilização de sessões protegidas com criptografia "ponta-a-ponta";

II - verificar a sua integridade e a do seu ambiente de execução, garantindo que o dispositivo utilizado pelo requerente esteja íntegro, sem indícios de desbloqueio de privilégios administrativos do sistema operacional, devendo tal condição ser verificada por mecanismos técnicos automáticos;

III - garantir que a identidade do dispositivo móvel do requerente seja única, imutável e atestada por elemento identificador de *hardware*;

IV - possibilitar a captura em tempo real de imagens;

V - possibilitar a captura da fotografia do documento identificação físico;

VI - possibilitar a captura das biometrias facial e de impressão digital ou ambas;

VII - permitir a detecção obrigatória de vivacidade (*liveness*) do requerente para minimizar manipulação de rosto e voz em montagens de vídeo conhecidas como "deepfake", com o emprego de meios de detecção de ataque de apresentação para garantir que a biometria utilizada para a identificação seja de uma pessoa viva presente no momento da prova de identidade e que não se trata de um fraudador;

VIII - aplicar meios de prevenção e detecção de ataques de injeção biométrica para assegurar que nem o requerente nem um atacante externo possam injetar, de forma indetectável, um fluxo de vídeo previamente gravado ou artificialmente gerado; e

IX - ser testada periodicamente por entidades independentes, de modo a avaliar o desempenho e efetividade das tecnologias de detecção de ataque de apresentação.

Parágrafo único. Na impossibilidade de realização de detecção de vivacidade, conforme disposto no inciso VII, do caput, o requerente deve ser direcionado para outra modalidade de emissão de certificado, por meio da qual seja possível a coleta da biometria da impressão digital.

Art. 58. O processo de emissão por AR Eletrônica deve compreender, no mínimo:

I - a autorização expressa do requerente para todo o processo de identificação, incluindo a captura de fotografias, imagens, documentos de identificação, a submissão de verificação biométrica e a inclusão de todas as informações e arquivos em dossiê eletrônico do titular do certificado.

II - a validação automática do documento de identificação físico em aplicativos e bases oficiais;

III - o batimento biométrico positivo em base de dados da Carteira Nacional de Identidade - CIN, da Identificação Civil Nacional - ICN ou da Infraestrutura Pública Digital - IPD de Identificação Civil;

IV - a observância dos critérios mínimos de aceitação da verificação biométrica e biográfica, nos termos do §3º do art. 39 deste Regulamento, admitindo-se exclusivamente o conceito equivalente a altíssima probabilidade; e

V - o batimento negativo na lista negativa do PSBio.

§1º Para os documentos mencionados no inciso II do caput, que contenham tecnologias verificáveis, como QR Code, MRZ, NFC, Chip ou similares, a validação do código ou tecnologia embarcada deverá ser realizada por meio de leitura automatizada.

§2º O batimento biométrico de que trata o inciso III do caput pode ser substituído pelo batimento positivo na base de dados da Carteira Nacional de Habilitação, por meio do Dataválid, combinado com o batimento biométrico positivo no PSBio, até que uma das bases de dados nele previstas esteja disponível em âmbito nacional.

§3º Quando a identificação do requerente, na modalidade AR Eletrônica, for realizada com a leitura e verificação automatizada dos dados biográficos e biométricos obtidos do Passaporte Eletrônico Brasileiro, ficam dispensados os incisos II e III do caput.

Art. 59. Todo o processo referente à emissão por AR Eletrônica deverá ser encadeado, assinado digitalmente, armazenado em repositório seguro e auditável.

#### CAPÍTULO VI DA COMUNICAÇÃO DE OCORRÊNCIA DE FRAUDE OU INDÍCIO

Art. 60. Quando a AR ou a AC concluir ter ocorrido fraude ou tentativa de fraude na identificação biométrica e na emissão de certificados digitais, deve comunicar tal fato ao ITI, mediante o procedimento descrito neste Capítulo e a prestação de informações constantes no adendo Métodos de Interface do Serviço de Lista Negativa (ADE-ICP-05.02.B), disponível no site do ITI.

Art. 61. A comunicação de fraude ou tentativa de fraude deve ser realizada por meio do preenchimento de campos obrigatórios e opcionais, dispostos 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.

§1º No momento do preenchimento dos campos na interface do sistema de comunicação de fraude, poderá ser requerido o *upload* de imagens específicas dos supostos fraudadores.

§2º As impressões digitais e a face devem ser enviadas pela AC ou PSS ao seu Sistema Biométrico para inserção dessas biometrias no respectivo repositório de Lista Negativa biométrica.

§3º As informações prestadas durante o preenchimento dos campos referentes às características dos supostos fraudadores devem retratá-los o mais fidedignamente possível.

§4º As informações mencionadas no §3º serão utilizadas posteriormente por todas as ACs para as pesquisas por características físicas na Lista Negativa da AC, sendo fundamental que estejam corretas para que se tornem eficientes.

Art. 62. Após o preenchimento dos campos do comunicado e *upload* das imagens, deve-se fazer uma verificação de todas as informações inseridas e, caso estejam corretas, deve ser enviado o comunicado ao ITI, conforme descrito no ADE-ICP-05.02.B.

Art. 63. Qualquer cancelamento de fraude, feito pelas ACs por processos de auditoria e análise detalhada, deve ser enviado ao endereço de correio eletrônico [comunicafrude@iti.gov.br](mailto:comunicafrude@iti.gov.br) com a descrição detalhada dos motivos do cancelamento.



Art. 64. A AC emissora do certificado digital deve notificar, ou cuidar para que se notifique a ocorrência de fraude à autoridade policial competente mais próxima do ocorrido.

Art. 65. Após o registro na Lista Negativa, o dossiê de emissão do certificado, os dossiês dos AGRs que atuaram na identificação do requerente e a cópia do Boletim de Ocorrência devem ser encaminhados ao ITI, aos cuidados da Diretoria de Auditoria, Fiscalização e Normalização - DAFN.

#### CAPÍTULO VII DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 66. As ACs devem realizar a pós-verificação dos certificados emitidos, de forma aleatória e distribuída entre os tipos de emissão e os tipos de certificados.

Art. 67. Todos os Prestadores de Serviços de Certificação - PSCert que tiverem acesso aos dados do requerente devem cumprir todas as disposições legais relativas à Lei Geral de Proteção de Dados - LGPD.

Art. 68. A atualização biométrica prevista no § 3º do art. 25 deste Regulamento torna-se obrigatória após 90 (noventa) dias da entrada em vigor desta Instrução Normativa.

Art. 69. Os mecanismos de segurança referentes à videoconferência, previstos nos incisos II e III do §1º do art. 37 deste Regulamento, passam a ser exigíveis após 90 (noventa) dias da entrada em vigor desta Instrução Normativa.

Art. 70. A utilização de documento físico na emissão por videoconferência, nos termos dos incisos I e III do art. 38 deste Regulamento, passa a ser obrigatória após 90 (noventa) dias da entrada em vigor desta Instrução Normativa.

Art. 71. As entidades da ICP-Brasil devem atualizar suas Declarações de Práticas de Certificação - DPCs e Políticas de Certificados - PCs, em conformidade com a Instrução Normativa nº 03, de 3 de abril de 2020, no prazo de até 60 (sessenta) dias, contados da entrada em vigor desta Instrução Normativa.

Art. 72. Ficam revogados:

I - a Instrução Normativa ITI nº 16, de 17 de novembro de 2020;

II - o artigo 1º da Instrução Normativa ITI nº 05, de 22 de fevereiro de 2021;

III - os incisos I e II do artigo 4º da Instrução Normativa ITI nº 05, de 22 de fevereiro de 2021; e

IV - a Instrução Normativa ITI nº 23, de 23 de março de 2022.

Art. 73. Esta Instrução Normativa entra em vigor em 05 de maio de 2026.

ENYLSON FLAVIO MARTINEZ CAMOLESI

#### INSTRUÇÃO NORMATIVA ITI Nº 37, DE 29 DE ABRIL DE 2026

Altera o Anexo da Instrução Normativa ITI nº 09, de 22 de outubro de 2020, que consolidou os Procedimentos para Identificação Biométrica na ICP-Brasil (DOC-ICP-05.03).

**O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO**, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 13 do anexo I do Decreto nº 12.103, de 8 de julho de 2024, 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, resolve:

Art. 1º 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:

"1.2 .....

a) AR: Autoridade de Registro responsável pela identificação do requerente de um certificado digital. Entre outros procedimentos de identificação, deve coletar e submeter à AC uma ou mais biometrias para permitir a validação ou cadastro de uma biometria na Rede PSBio e verificação em Base Oficial Nacional;

..... " (NR)

"2.4.2.....

a).....

d) verificação de qualidade e quantidade de minúcias da impressão digital baseada no padrão NFIQ 2.0 (aceitar score igual ou superior a 70), medida após a compressão WSQ;

..... " (NR)

"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 em instrução normativa da AC Raiz, 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.

2.5.4.2 A emissão do certificado está condicionada à validação dos dados biométricos na base do PSBio ou em seu cache.

2.6.....

2.6.1.....

2.6.5 As ACs farão uso do capítulo sobre comunicação de ocorrência de fraude ou indício da Instrução Normativa da AC Raiz que estabelece requisitos e procedimentos para a confirmação da identidade de requerente de certificado digital no âmbito da ICP-Brasil para encaminhar os dados biométricos de um suposto fraudador à AC Raiz.

2.6.6 Em caso de confirmação de fraude após análise, a AC responsável pelo cadastro (IDN) deve informar ao PSBio a necessidade de remoção do IDN da base, quando aplicável. O PSBio deverá fazer a propagação da mensagem de remoção à Rede PSBio. Devem ainda ser adotados os procedimentos de fraude conforme a Instrução Normativa da AC Raiz que estabelece requisitos e procedimentos para a confirmação da identidade de requerente de certificado digital no âmbito da ICP-Brasil.

..... " (NR)

"3.4.2 Cada PSBio credenciado na ICP-Brasil deverá realizar, obrigatoriamente, um processo de deduplicação semestral em sua base biométrica, com o objetivo de identificar e tratar registros duplicados ou inconsistentes. " (NR)

"3.6.3 .....

a) impressão digital (indexando um dedo): para FAR (false accept rate) de 0,01%, TAR (true accept rate) de, no mínimo, 99,0%.

b) impressão digital (indexando dois dedos): para FAR de 0,01%, TAR de, no mínimo, 99,4%.

c) impressão digital (indexando três ou quatro dedos): para FAR de 0,01%, TAR de, no mínimo, 99,8%.

d).....

..... " (NR)

"3.6.5 O PSBio que não atingir, no mês, o SLA (Service Level Agreement) estabelecido nos itens 3.6.1 a 3.6.4 fica impedido de prestar serviços para qualquer AC, inclusive à AC que o contratou, até a completa regularização, sem prejuízo das demais sanções aplicáveis. " (NR)

"3.13.1 A base de fraudadores será mantida atualizada através da consulta ao sistema SAF, conforme Instrução Normativa da AC Raiz que estabelece requisitos e procedimentos para a confirmação da identidade de requerente de certificado digital no âmbito da ICP-Brasil. " (NR)

"4.....

4.1.2.....

a) na modalidade presencial, mantém-se a coleta de face e impressões digitais do requerente, conforme estabelecido neste documento;

b) nas modalidades de videoconferência, Módulo Eletrônico de AR e AR Eletrônica, com batimento biométrico em Base Oficial Nacional, admite-se somente a face ou impressões digitais e face do requerente, conforme estabelecido neste documento. " (NR)

"4.1.6.....

4.1.6.1 As ACs deverão realizar captura antecipada de minúcias biométricas (face e impressão digital) possibilitando ao usuário a coleta biométrica antes de iniciar a emissão do certificado na modalidade de videoconferência com batimento biométrico em base oficial nacional ou na verificação na rede PSBio. (NR)

Art. 2º Fica aprovada a versão 4.0 do Documento Procedimentos para Identificação Biométrica na ICP-Brasil (DOC-ICP-05.03);

Parágrafo único. A identificação da versão do DOC-ICP-05.03 deverá ser atualizada no preâmbulo e incluída no controle de versões do anexo da Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

Art. 3º Fica revogado o item 1.5 do Anexo da Instrução Normativa ITI nº 09, de 22 de outubro de 2020.

Art. 4º Esta Instrução Normativa entra em vigor em 05 de maio de 2026.

ENYLSON FLAVIO MARTINEZ CAMOLESI

#### SECRETARIA-GERAL

#### PORTARIA INTERMINISTERIAL SG-PR/MEC/MDS Nº 213, DE 30 DE ABRIL DE 2026

Institui a Plataforma Juventude Solidária e dá outras providências.

**O MINISTRO DE ESTADO DA SECRETARIA-GERAL DA PRESIDÊNCIA DA REPÚBLICA, O MINISTRO DE ESTADO DA EDUCAÇÃO E O MINISTRO DE ESTADO DO DESENVOLVIMENTO E ASSISTÊNCIA SOCIAL, FAMÍLIA E COMBATE À FOME SUBSTITUTO**, no uso da atribuição que lhes confere o art. 87, parágrafo único, incisos II e IV, da Constituição Federal, e tendo em vista o disposto na Lei nº 12.852, de 5 de agosto de 2013, resolvem:

Art. 1º Fica instituída a Plataforma Juventude Solidária, com a finalidade de articular e organizar ações de voluntariado juvenil, voltadas à promoção da cidadania ativa.

Parágrafo único. A Plataforma Juventude Solidária compreende o conjunto de ações e iniciativas de promoção do voluntariado juvenil, integrando-se ao Sistema Nacional de Juventude (Sinajuve) e à Plataforma Brasil Participativo, com o objetivo de conectar jovens com idade entre dezesseis e vinte e nove anos, organizações da sociedade civil e órgãos e entidades da administração pública promotores de políticas públicas responsáveis pela execução de programas sociais em curso.

Art. 2º São princípios da Plataforma Juventude Solidária:

I - promoção da participação social da juventude;

II - valorização do voluntariado juvenil;

III - intersetorialidade das ações governamentais;

IV - respeito à diversidade e à interculturalidade;

V - transparência e publicidade dos procedimentos;

VI - sustentabilidade das ações desenvolvidas; e

VII - coordenação das ações entre os entes federativos, consideradas as realidades dos territórios de atuação.

Art. 3º São objetivos da Plataforma Juventude Solidária:

I - promover a participação social da juventude, por meio de ações de voluntariado relacionadas a programas sociais existentes;

II - articular organizações da sociedade civil, comunidades e jovens voluntários, com vistas ao desenvolvimento de ações de interesse público;

III - favorecer a integração de políticas públicas setoriais;

IV - estimular a continuidade das ações apoiadas, por meio do fortalecimento de redes locais e de mecanismos de participação social; e

V - contribuir para a redução de desigualdades territoriais, no âmbito das ações desenvolvidas.

Art. 4º Poderão inscrever projetos na Plataforma Juventude Solidária as organizações da sociedade civil que:

I - atuem em territórios caracterizados por vulnerabilidade social;

II - prestem apoio voluntário no âmbito das ações propostas; e

III - observem os critérios objetivos definidos em chamamento público.

Parágrafo único. As organizações da sociedade civil selecionadas poderão receber recursos para o custeio de despesas necessárias à execução dos projetos, observadas as normas aplicáveis.

Art. 5º Poderão inscrever projetos na Plataforma Juventude Solidária os órgãos ou entidades da administração pública que:

I - disponham de equipamentos públicos ou atuem em territórios caracterizados por vulnerabilidade social;

II - ofertem ações de interesse público com participação de jovens voluntários; e

III - observem os critérios objetivos definidos em chamamento público.

Parágrafo único. Os órgãos ou entidades da administração pública selecionados poderão receber recursos para custeio de despesas necessárias à execução dos projetos, observadas as normas aplicáveis.

Art. 6º Poderão se inscrever como voluntários na Plataforma Juventude Solidária jovens com idade entre dezesseis e vinte e nove anos, desde que atendidos os requisitos e critérios objetivos estabelecidos em chamamento público.

§1º A participação na Plataforma configura-se como atividade de voluntariado, nos termos da Lei nº 9.608, de 18 de fevereiro de 1998, ficando condicionada à efetiva execução das atividades previstas no projeto ao qual o voluntário esteja vinculado, observadas as atribuições, a carga horária e o acompanhamento institucional nele definidos.

§2º Os voluntários selecionados que estiverem inscritos no Programa Identidade Jovem - ID JOVEM poderão receber ajuda de custo, observados os critérios objetivos previamente estabelecidos em chamamento público, destinada ao custeio de despesas necessárias à participação nas atividades de voluntariado.

§3º O voluntário que deixar de cumprir as obrigações previstas no projeto ao qual esteja vinculado, será desligado da iniciativa pela coordenação responsável, hipótese em que não fará jus à percepção da ajuda de custo de que trata o § 2º.

Art. 7º A Coordenação Nacional da Plataforma Juventude Solidária caberá à Secretaria Nacional de Juventude da Secretaria-Geral da Presidência da República.

Parágrafo único. Compete à Coordenação Nacional da Plataforma:

I - coordenar a execução das ações centrais da Plataforma; e

II - exercer a secretaria-executiva do Comitê Gestor da Plataforma Juventude Solidária.

Art. 8º O Comitê Gestor da Plataforma Juventude Solidária será composto por representantes dos seguintes Ministérios:

I - Secretaria-Geral da Presidência da República, que o presidirá;

II - Ministério da Educação; e

III - Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome.

§1º Os representantes do Comitê Gestor serão indicados pelos titulares dos respectivos órgãos e designados por ato do Ministro de Estado da Secretaria-Geral da Presidência da República.

