



Procedimento Operacional Padrão - POP

Aprovação de certificados digitais para Pessoas
Físicas na AC-JUS

2023

SUPOP/OPCDI/OPPAR
Setembro/2023

Sumário

| | |
|---|-----------|
| CONTROLE DE VERSÕES..... | 2 |
| RESUMO DO DOCUMENTO..... | 2 |
| 1. Considerações sobre Certificados na AC-JUS..... | 3 |
| 2 - Cadastramento de Órgãos não pertencentes ao Poder Judiciário..... | 4 |
| 3 - Autorização..... | 5 |
| 4 - Sobre tipos de certificados:..... | 6 |
| 4.1 - Leiaute do Certificado AC-JUS Institucional..... | 6 |
| 4.2 - Leiaute do Certificado AC-JUS Magistrado..... | 6 |
| 4.3 - Leiaute do Certificado AC-JUS Poder Público..... | 7 |
| 4.4 - Leiaute do Certificado AC-JUS Aplicação..... | 8 |
| 4.5 - Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS (após 2018)..... | 8 |
| 5. Considerações Gerais sobre documentação..... | 9 |
| 5.1 - Documentação da Pessoa Física para a AC-JUS..... | 9 |
| 5.1.1 - Autorização..... | 9 |
| 5.1.2 - Documento de identificação original (válido em todo o território nacional com assinatura e foto) - OBRIGATÓRIO..... | 9 |
| 5.1.3 - CPF - OBRIGATÓRIO..... | 10 |
| 5.1.4 - Termo de Titularidade..... | 11 |
| 5.1.5 - CEI (quando informado na solicitação)..... | 11 |
| 5.1.6 - NIT/NIS/PIS/PASEP (quando informado na solicitação)..... | 11 |
| 5.1.7 - Título de Eleitor (quando informado na solicitação)..... | 11 |
| 6 - Identificação da Pessoa Física..... | 11 |
| 7 - Validação do Termo de Titularidade..... | 12 |
| 8 - Validação Sistematizada..... | 12 |
| 9 - Aprovação no SCDS..... | 13 |
| 10 - Revogação de Certificados..... | 14 |
| 11 - Resumo das fases de aprovação de certificados digitais..... | 14 |

CONTROLE DE VERSÕES

| Versão | Data | Autor/Revisor | Status do documento | Versões de alterações |
|--------|------------|---|---------------------|-----------------------|
| 1.0 | 15/09/2023 | Juliana Cristina de Oliveira e Eliana Dias Rosa | Criação | Versão original |

RESUMO DO DOCUMENTO

| | |
|----------------------|---|
| Descrição: | Este Procedimento Operacional Padrão orienta os Agentes de Registro sobre os documentos aceitos e as verificações necessárias pra emissão do Certificado Digital na AC-JUS. Neste documento são definidos os campos, extensões e informações obrigatórias que devem constar em cada perfil de certificado especificado, bem como as regras, restrições e requisitos documentais para emissão dos certificados sob a cadeia de certificação da AC-JUS. |
| Local de Publicação: | https://diope.serpro/supop/corporativo/produtos-servicos/servico-certificacao-digital/area-do-agente-de-registro/procedimentos-dos-agrs/procedimento-operacional-padrao-pop/pop-procedimento-operacional-padrao-pf-cert-jus-v1-0-setembro_2023/view |

1. Considerações sobre Certificados na AC-JUS

Os certificados digitais AC-JUS destinam-se a servidores, magistrados e aplicações, dos órgãos do Poder Judiciário e da Administração Pública direta e indireta. Cada certificado digital identifica seu titular ou aplicação, relacionando-os a determinado órgão público ou ao Poder Judiciário no caso do certificado AC-JUS Magistrado.

O órgão público que desejar fazer uso dos certificados digitais AC-JUS, deve autorizar a emissão para cada titular, equipamento ou aplicação e é responsável pelo fornecimento das informações funcionais e institucionais que devem constar no certificado digital.

O órgão é responsável também, por garantir a revogação do certificado digital ou a destruição da sua chave privada em caso de desligamento do titular do certificado.

No caso de certificados digitais emitidos para Magistrados, não se faz necessária a revogação em caso de mudança de jurisdição ou atuação em outro órgão.

Por força da Resolução CNJ n. 376, de 02 de março de 2021, passa a ser obrigatório uso da flexão de gênero no campo cargo dos Certificados AC-JUS Institucional e AC-JUS Magistrado.

1.1 - Para o disposto neste documento, entende-se como autoridade competente:

- a autoridade máxima do órgão;
- o representante legal do órgão ou pessoa com delegação formal para representação administrativa do órgão;
- servidores com responsabilidade delegada para representação administrativa do órgão por meio de ato oficial ou pela natureza de suas atribuições, descritas em regimento interno ou semelhante;
- servidores designados para esta finalidade, por meio de ato oficial;
- recomenda-se a designação pelo órgão, dos servidores que responsáveis pela autorização no início da execução contratual, com renovação anual da designação.

1.2 - Os certificados emitidos sob a cadeia AC-JUS seguem os padrões definidos pela ICP-Brasil e obedecem às premissas de conformidade e interoperabilidade estabelecidas nas resoluções e normas da ICP-Brasil e da AC-Raiz.

1.3 - As autoridades certificadoras da cadeia de certificação da AC-JUS somente emitirão certificados que possuam leiaute e conteúdo conforme definido neste documento.

1.4 - As autoridades certificadoras da cadeia de certificação da AC-JUS somente emitirão certificados digitais AC-JUS para os órgãos previamente cadastrados junto à AC-JUS conforme o item 4.

1.5 - Todos os órgãos autorizados a utilizarem certificados digitais AC-JUS estão relacionados no documento Lista de Órgãos Autorizados – AC-JUS, disponível no site da AC-JUS em <http://www.acjus.jus.br/>

1.6 - Não é permitida a emissão de certificado digitais de SSL/TLS, Codesigning, Sigilo e CF e-SAT na cadeia da AC-JUS.

2 - Cadastramento de Órgãos não pertencentes ao Poder Judiciário

A AC-JUS definiu um perfil de certificado digital específico, chamado AC-JUS Poder Público, para ser utilizado por órgãos da Administração Pública direta e indireta, não pertencentes ao Poder Judiciário.

O modelo AC-JUS Aplicação pode ser utilizado por todos os órgãos cadastrados.

Órgãos não pertencentes ao Poder Judiciário deverão solicitar CADASTRAMENTO junto à AC-JUS, para se habilitarem à emissão de certificados digitais AC-JUS.

As AC da cadeia AC-JUS somente emitirão certificados digitais para órgãos não pertencentes ao Poder Judiciário após o CADASTRAMENTO ter sido aprovado pela AC-JUS.

O cadastramento deve ser solicitado por ofício da autoridade competente do órgão interessado, endereçado à AC-JUS.

Após a aprovação do cadastro a AC-JUS oficiará as AC subsequentes para que incluam o órgão cadastrado nos seus sistemas de certificação.

A lista de órgãos cadastrados, bem como as respectivas siglas padronizadas, está publicada no repositório da AC-JUS e é divulgada para todas as Autoridades Certificadoras da cadeia AC-JUS.

Em caso de dúvida sobre a padronização de nomes ou siglas, ou órgãos não constantes da lista publicada, a unidade administrativa da AC-JUS deve ser consultada.

Os órgãos do Poder Judiciário não necessitam fazer cadastramento desde que já constem na Lista de órgãos autorizados, distribuída às Autoridades Certificadoras e publicada no site da AC-JUS.

3 - Autorização

Para a emissão de qualquer certificado digital AC-JUS é necessária autorização da autoridade competente da instituição ou órgão à qual o titular do certificado está relacionado.

A autorização conterá todas as informações institucionais obrigatórias, necessárias para a emissão do certificado digital, conforme cada leiaute definido, além dos campos opcionais de interesse da instituição.

As informações de lotação, cargo, matrícula e e-mail institucional, devem, obrigatoriamente, constar na AUTORIZAÇÃO.

A informação do UPN é opcional somente para o tipo de Certificado Poder Público.

Cada órgão autorizado pela AC-JUS a emitir certificados digitais **AC-JUS Poder Público** poderá fazer acordos com as Autoridades Certificadoras da Cadeia AC-JUS para padronização do campo cargo, facilitando assim o processo de emissão dos certificados digitais.

A AC-JUS mantém em seu sítio em <http://www.acjus.jus.br>, modelos de AUTORIZAÇÃO para diversos tipos de certificado.

As autorizações para emissão de certificados, não necessitam ser individualizadas. Podem ser utilizadas listas ou outros meios acordados entre o órgão e a Autoridade Certificadora emitente, desde que sejam assinadas digitalmente pela autoridade competente ou pelo responsável que tenha uma outorga da autoridade competente especificamente para essa autorização e contenham todas as informações institucionais requeridas. (Ver item 1.1)

Para AR SERPRO além do documento de autorização assinado digitalmente o autorizador cadastrado no sistema agenda deverá cadastrar no sistema Agenda certificados a autorização para uso do contrato.

4 - Sobre tipos de certificados:

4.1 - Leiaute do Certificado AC-JUS Institucional

O certificado digital AC-JUS Institucional deve ser do tipo A3 ou superior.

Para os certificados A3 ou superior, deverá ser utilizado dispositivo criptográfico para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado admitida a modalidade de certificado em nuvem.

A validade de certificados será de no máximo 3 anos.

Destinação

Os certificados digitais AC-JUS Institucional destinam-se exclusivamente aos agentes públicos do Poder Judiciário, autorizados pela autoridade competente do seu órgão de lotação a recebê-los. Identificam os titulares do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.

Os certificados digitais AC-JUS Institucional NÃO PODERÃO mais ser emitidos para MAGISTRADOS do Poder Judiciário a partir de 1º de janeiro de 2021.

4.2 - Leiaute do Certificado AC-JUS Magistrado

O certificado digital AC-JUS Magistrado deve ser do tipo A3 ou superior e destina-se exclusivamente a Magistrados.

Para os certificados A3 ou superior, deverá ser utilizado dispositivo criptográfico para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado, admitida a modalidade de certificado em nuvem

A validade será de, no máximo, 5 anos.

Destinação

Os certificados digitais AC-JUS Magistrado destinam-se exclusivamente aos MAGISTRADOS do Poder Judiciário, autorizados pela autoridade competente do seu atual órgão de atuação a recebê-los. Identificam os titulares não só como indivíduos, mas também como Magistrados do Poder Judiciário.

4.3 - Leiaute do Certificado AC-JUS Poder Público

O certificado digital AC-JUS Poder Público deve preferencialmente ser do tipo A3 ou superior. Para os certificados A3 ou superior, deverá ser utilizado dispositivo criptográfico (ex.: token ou smartcard) para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.

A validade de certificados de no máximo 5 anos.

A emissão de certificados AC-JUS Poder Público para determinado órgão só será iniciada pela Autoridade Certificadora emitente, após o CADASTRAMENTO de que trata o item 2.

Destinação

Os certificados digitais AC-JUS Poder Público destinam-se exclusivamente a agentes públicos, autorizados pela autoridade competente do seu órgão de lotação, a recebê-los.

O certificado AC-JUS Poder Público identifica o titular do certificado não só como indivíduo, mas também como servidor do órgão público em que está lotado.

É vedada a emissão do AC-JUS Poder Público para servidores de órgãos do Poder Judiciário.

4.4 - Leiaute do Certificado AC-JUS Aplicação

Os certificados digitais AC-JUS Aplicação são certificados para pessoa jurídica destinados exclusivamente à utilização em aplicações que disponibilizem ou consumam serviços ou informações (OCSP, webservices, autenticação entre serviços e outras aplicações) que requeiram certificados digitais ICP-Brasil para autenticação e assinatura digital de pessoa jurídica. O certificado AC-JUS Aplicação poderá ser do tipo A1.

A emissão de certificados digitais AC-JUS Aplicação deve ser previamente autorizada pela autoridade competente do órgão.

O titular do certificado digital AC-JUS Aplicação será sempre um órgão público e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público indicado e autorizado pela autoridade competente.

A emissão de certificados digitais AC-JUS Aplicação para determinado órgão só será iniciado após o CADASTRAMENTO de que trata o item 1.5.

Certificados de resposta OCSP: Os certificados de resposta OCSP serão emitidos somente para autoridades certificadoras subsequentes à AC-JUS, pela própria AC subsequente, de forma viabilizar a autenticação do seu serviço OCSP. Para este certificado está dispensada a Autorização e o Cadastramento de que tratam os itens 4 e 5. O Leiaute desse tipo de certificado deve estar de acordo como os normativos da ICP-Brasil.

4.5 - Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS (após 2018)

Requisitos de Certificado

Os certificados emitidos pela AC-JUS para as Autoridades Certificadoras subsequentes obedecem ao formato definido no padrão internacional ITU-T X.509 ou ISO/IEC 9594-8 e implementam a versão 3 de certificado de acordo com o perfil estabelecido na RFC 5280 (Request for Comments – Internet X.509 Public Key Infrastructure).

Os certificados das AC subsequentes deverão atender aos demais requisitos definidos pela ICP-Brasil. Na cadeia AC-JUS serão emitidos somente certificados S/MIME.

5. Considerações Gerais sobre documentação

Para certificados de pessoa física é necessária a comprovação de que a pessoa física que se apresenta como titular do certificado é realmente aquela cujos dados constam na documentação, autorização e biometria coletada, vedada qualquer espécie de procuração para tal fim¹. A identificação da Pessoa Física deve ser feita presencialmente ou através de videoconferência.

1 [DOC-ICP-05](#), versão 5.4, item 3.2

5.1 - Documentação da Pessoa Física para a AC-JUS

5.1.1 - Autorização

Para a emissão de qualquer certificado digital AC-JUS é necessária autorização da autoridade competente da instituição ou órgão à qual o titular do certificado está relacionado.

As informações de lotação, cargo, matrícula e e-mail institucional, devem, obrigatoriamente, constar na AUTORIZAÇÃO.

A informação do UPN é opcional somente para o tipo de Certificado Poder Público.

A AC-JUS mantém em seu sítio em <http://www.acjus.jus.br>, modelos de AUTORIZAÇÃO para diversos tipos de certificado.

5.1.2 - Documento de identificação original (válido em todo o território nacional com assinatura e foto) - OBRIGATÓRIO

- Carteira Nacional de Habilitação – CNH
 - Pode ser aceita mesmo estando vencida
- Registro Geral – RG
 - Verificar se os dados impressos no documento estão legíveis e em perfeito estado
 - Verificar a semelhança da foto do documento com o solicitante presente
 - Rejeitar caso os itens acima não sejam atendidos
- Passaporte
 - Verificar prazo de validade

- Se estrangeiro não domiciliado no Brasil
- Deve possuir visto de permanência válido
- Carteira de Trabalho e Previdência Social – CTPS
 - Somente modelo com foto digitalizada em papel
- Carteiras de Órgãos de Classe
 - OAB, CRM, CFC, etc
- Carteira Funcional
 - Desde que contenha a validade em todo o território nacional, emitidos por força de lei e com fotografia.
- Registro Nacional de Estrangeiro – RNE / CNE
 - Se estrangeiro domiciliado no Brasil
 - Verificar prazo de validade
 - Se o portador completou 60 anos antes da data de vencimento ou é deficiente físico, pode ser aceita vencida.



Verificar se o nome constante do documento de identificação apresentado confere com o cadastro do CPF. Caso haja divergência, a mesma deve ser esclarecida e corrigida se necessário. Na situação de mudança do estado civil (casamento, divórcio, por exemplo) que impliquem alteração do nome, deve ser exigido documento que comprove a situação. Certidão de casamento, por exemplo.

5.1.3 - CPF - OBRIGATÓRIO

- Cartão do CPF ou
- Número presente no documento de identificação ou
- Consulta no site da Receita Federal do Brasil
 - Emitido no máximo há três meses
 - Pode ser levado pelo cliente ou consultado pelo AGR e gravado como PDF/Imagem(jpg)
 - Consulta disponível em:
<https://servicos.receita.fazenda.gov.br/Servicos/CPF/ConsultaSituacao/ConsultaPublica.asp>

5.1.4 - Termo de Titularidade

- O Termo de Titularidade para certificados Pessoa Física será assinado exclusivamente de forma eletrônica no momento da baixa/instalação do certificado.

5.1.5 - CEI (quando informado na solicitação)

- Comprovante de emissão emitido por
 - Receita Federal do Brasil, ou
 - Dataprev

5.1.6 - NIT/NIS/PIS/PASEP (quando informado na solicitação)

- Apresentar
 - Cartão do Cidadão, ou
 - Declaração da Caixa Econômica Federal, ou ▪ Carteira de Trabalho com o número, ou ▪ Consulta disponível em:
<http://consultacadastral.inss.gov.br/Esocial/pages/qualificacao/qualificar.xhtml>

5.1.7 - Título de Eleitor (quando informado na solicitação)

- Apresentar
 - Documento emitido pelo TSE ou ▪ Consulta no site do TSE, disponível em: <http://www.tse.jus.br/eleitor/certidoes/certidao-de-quitacao-eleitoral>

6 - Identificação da Pessoa Física

- Com o documento de identificação fazer a validação da pessoa física, verificar:
 - Se a imagem contida no documento apresentado corresponde à pessoa que está se apresentando pessoalmente ou por meio de videoconferência para a emissão do certificado digital;
 - Se a imagem no documento corresponde à idade aparente no momento em que o documento foi emitido (idade resultante da diferença entre a data de nascimento e data de emissão do documento);
 - Se a idade atual coincide com a aparência atual da pessoa.



Como o Termo de Titularidade para certificados de Pessoa Física é assinado exclusivamente de modo eletrônico não há mais a verificação de assinatura manuscrita.

7 - Validação do Termo de Titularidade

- Comparar documentos originais e os dados da autorização com o Termo de Titularidade:
 - Nome
 - Data de Nascimento
 - CPF
 - E-mail institucional, Matrícula e Cargo, conforme a autorização.
 - RG / Órgão Emissor / UF (quando informado)
 - deve estar preenchido somente com número de RG civil. Não deve conter RG militar, números de CNH, Carteiras de Classe, etc.
 - Título de Eleitor (quando informado verificar Número, Zona, Seção Município e UF)
 - NIT/NIS/PASEP (quando informado)
 - CEI (quando informado)

8 - Validação Sistematizada

- Validação de documento(s) do solicitante:
 - Bases Oficiais

O SCDS realizará uma verificação automática nas bases de dados oficiais usando o CPF como referência. O resultado será a porcentagem de semelhança ao comparar as faces apresentadas durante a videoconferência e/ou coleta biométrica presencial com a face registrada nas bases oficiais. Se houver discrepâncias nas informações, o Agente de Registro (AGR) não deve continuar com o processo de aprovação.

- Realizar consulta no sistema antifraude ITI
 - O SCDS realizará automaticamente consulta à base do SAF – Sistema AntiFraude e trará o resultado desta consulta na tela para o AGR.
 - Não havendo ocorrência, prosseguir com as etapas seguintes;
 - Caso o sistema sinalize alguma ocorrência, o AGR deverá pausar o processo de aprovação, acessar o SAF pelo endereço <https://saf.serpro.gov.br> (vide manual específico do SAF) e:
 - Verificar se a foto do solicitante consta nas imagens das faces dos maiores fraudadores;
 - Verificar as últimas ocorrências incluídas no sistema (clicar no ícone da "lâmpada");
 - Realizar pesquisa única – informando os seguintes dados: Nome, CPF e E-mail;
 - Usando SEMPRE a forma de busca “RESULTADO – QUALQUER CAMPO”
 - Se a identificação facial for positiva em alguma das pesquisas, é necessário suspender imediatamente o processo de emissão do certificado digital. Deve-se conduzir uma análise em conjunto com a Autoridade Certificadora (AC) vinculada, comunicando-a sobre essa suspeita. Se a tentativa de fraude for confirmada, a emissão do certificado digital não deve ocorrer, e é imperativo comunicar imediatamente ao Instituto Nacional de Tecnologia da Informação (ITI) por meio do SAF, seguindo o procedimento do item "Cadastrar Ocorrência". No caso em que a identificação facial não tenha sido encontrada, todos os procedimentos estipulados pelas normas da ICP-Brasil para a verificação documental do solicitante devem continuar vigentes e serem rigorosamente executados.
 - Para outras ações relacionadas a casos em que o solicitante esteja na lista negativa, siga as orientações contidas no [POP - Procedimento Operacional Padrão SAF](#)

9 - Aprovação no SCDS

- Após a conclusão das etapas de verificação e validação dos documentos, bem como da autorização com base nos documentos apresentados, proceder com a aprovação do certificado digital.

10 - Revogação de Certificados

Os certificados digitais Cert -JUS Institucional e Poder Público, devido à sua natureza especial, que vincula o titular do certificado a determinada instituição, podem ser revogados a pedido da instituição ou órgão de lotação do titular do certificado.

É obrigação do titular solicitar a revogação do certificado digital quando for desligado do quadro funcional do órgão que autorizou a emissão do certificado.

Cabe à instituição ou órgão de lotação do titular de um certificado digital AC-JUS, garantir a revogação do certificado se aquele titular não mais fizer parte dos seus quadros ou em caso de alteração de alguma informação contida no certificado.

Para certificados digitais emitidos para Magistrados, não se faz necessária a revogação em caso de mudança de jurisdição ou atuação em outro órgão.

11 - Resumo das fases de aprovação de certificados digitais

1. AGR recebe a documentação do usuário com o(s) número(s) do(s) pedido(s) de cada certificado e faz a verificação se os dados do(s) pedido(s) conferem com os dados dos documentos apresentados, solicitando a correção se necessário;
2. Realiza entrevista (presencial ou por videoconferência);
3. Se for presencial, AGR faz a Validação Biométrica (Cadastro, Verificação ou Atualização);
4. Se for por videoconferência, além dos procedimentos previstos, durante o processo, o AGR realiza a captura da imagem da face do usuário;
5. AGR prossegue com o processo de validação e aprovação conforme descrito no **item IV Atividades do AGR do Manual Operacional do Agente de Registro**;
6. Para certificados do tipo Aplicação a assinatura do Termo de Titularidade deverá ser manuscrita na presença do AGR caso a identificação seja presencial. No caso de atendimento por videoconferência, o AGR deve garantir que o termo seja assinado digitalmente pelo Titular e Responsável. O(s) AGR(s) devem também apor a respectiva assinatura digital no documento.
7. Após a aprovação, o AGR deve fazer o upload de todos os documentos necessários na seção “Dossiê” do SCDS, classificando e assinando-os digitalmente.