INSTITUTO DE PESQUISAS JARDIM BOTÂNICO DO RJ

Estudo Técnico Preliminar 83/2025

1. Informações Básicas

Número do processo: 02011.000149/2026-32

2. Descrição da necessidade

1.1. Este estudo é feito em atendimento à Instrução Normativa nº 94, de 23 de dezembro de 2022, da Secretaria de Governo Digital do Ministério da Economia, e a Instrução Normativa nº 40, de 22 de maio de 2020, Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, para atendimento a contratação de empresa para emissão de certificados digitais A3, na nuvem, pessoa física.

1.2. As contratações de serviços para aquisição de certificados digitais A3, na nuvem, pessoa física, e certificados digitais A3 com dispositivo token USB pessoa física devem ser precedidas de Estudos Técnicos Preliminares para análise da sua viabilidade e o levantamento dos elementos essenciais que servirão para compor o Termo de Referência, de forma que melhor atenda às necessidades da Administração.

1.3. O objetivo deste estudo é fornecer uma análise detalhada dos serviços de aquisição de certificados digitais A3, na nuvem, pessoa física, e certificados digitais A3 com dispositivo token USB pessoa física, com foco em desempenho, compatibilidade e custo-benefício, para suportar a decisão de contratação desses serviços.

1.4. A presente demanda tem por objetivo, garantir a autenticidade, integridade e validade jurídica de documentos eletrônicos, bem como permitir o acesso seguro a sistemas governamentais como SEI, Compras.gov.br, Sigepe, SouGov, eSocial, Gov.br, entre outros.

1.5. O Instituto de Pesquisas Jardim Botânico do Rio de Janeiro (JBRJ) tem por objetivo contratar uma empresa especializada nos serviços de emissão de certificados digitais A3, na nuvem, pessoa física, e certificados digitais A3 com dispositivo token USB pessoa física, destinados aos servidores que desempenham atividades administrativas e técnicas que demandam assinatura digital com validade jurídica, assegurando a autenticidade, integridade e confiabilidade dos atos eletrônicos praticados no âmbito institucional.

1.6. A contratação atende às exigências legais de digitalização e transformação digital da Administração Pública, alinhando-se às diretrizes de eficiência, economicidade e sustentabilidade no uso dos recursos públicos.

1.7. Inicialmente, foi instruído procedimento somente para contratação de Certificado Digital A3 com fornecimento de token USB. Contudo, quando os autos foram submetidos à apreciação da Diretoria, houve devolução para reavaliação, com orientação expressa no sentido de observar as diretrizes que ressaltam a necessidade de que os certificados digitais sejam emitidos por Autoridades Certificadoras vinculadas ao Governo.

1.8. Diante da referida orientação, em 09 de fevereiro de 2026, foi solicitada cotação ao Serviço Federal de Processamento de Dados (Serpro), por se tratar de Autoridade Certificadora integrante da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e vinculada ao Governo Federal.

1.9. Em contato telefônico, o Serpro informou que o modelo de Certificado Digital A3 em nuvem apresenta-se mais vantajoso e prático em comparação ao modelo com token físico, tendo em vista que a validação das assinaturas é realizada por meio de dispositivo móvel (aplicativo no celular), dispensando o uso de token USB. Tal solução reduz o risco de extravio ou dano de dispositivo físico, além de proporcionar maior mobilidade e facilidade de utilização.

1.9. A proposta comercial foi encaminhada pelo Serpro em 03/03/2026, passando o processo a tramitar com base na solução de certificado digital A3 em nuvem, em conformidade com as orientações superiores.

1.10. Porém após o envio do processo para realização da dipensa, a diretoria nos devolveu para adequação, a fim de contemplar os modelos de certificados digitais necessários à contratação.

1.11. A referida adequação justifica-se pela necessidade de previsão de ambos os modelos de certificação, tendo em vista que determinados sistemas exigem a utilização de certificado em dispositivo criptográfico físico (token), enquanto outros admitem a utilização de certificado em nuvem. Dessa forma, a contratação de apenas um dos modelos não atenderia integralmente às demandas institucionais.

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Tecnologia da Informação e Comunicação	Bruno Augusto de Farias

4. Necessidades de Negócio

4.1. As necessidades de negócio referem-se às demandas institucionais que impulsionam a contratação do serviço e estão diretamente relacionadas à missão do JBRJ como instituição pública voltada à pesquisa, conservação da biodiversidade e prestação de serviços ao cidadão. Nesse contexto, são destacadas:

4.1.1. Garantir a continuidade das atividades administrativas e técnicas que dependem de certificação digital para tramitação de processos eletrônicos.

4.1.2. Aprimorar a segurança da informação, evitando fraudes e assegurando a integridade dos atos administrativos.

4.1.3. Assegurar autonomia operacional dos servidores do JBRJ no uso de certificados pessoais para autenticação e assinatura de documentos oficiais.

5. Necessidades Tecnológicas

5.1. As necessidades tecnológicas envolvem os recursos e condições técnicas mínimas exigidas para atender às demandas institucionais com segurança, qualidade e eficiência. São elas:

5.1.1. Certificados digitais padrão ICP-Brasil, tipo A3 (armazenamento criptográfico em dispositivo físico).

5.1.2. Dispositivos (tokens) compatíveis com os sistemas operacionais Windows, Linux e macOS.

5.1.3. Validade mínima de 36 (trinta e seis) meses, para cada dispositivo, e 36 meses de contrato, renovável por mais 36 meses.

5.1.4. Suporte técnico para instalação e configuração dos certificados e tokens.

5.1.5. Emissão e renovação realizadas de forma presencial ou remota, conforme regulamentação da ICP-Brasil.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1. Os certificados a serem disponibilizados para uso devem atender aos seguintes requisitos:

6.2. Os certificados devem estar conformes às políticas da ICP-Brasil e emitidos por Autoridades Certificadoras credenciadas.

6.3. A solução deve prever suporte técnico e garantia durante o período de validade do certificado.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A demanda atual identificada pelo JBRJ corresponde a:

Item	Descrição	Quantidade	Validade
1	Certificados Digitais A3 - e - CPF, com dispositivo Token USB	20 unidades	36 meses para cada dispositivo, e 36 meses de contrato, renovável por mais 36 meses.
2	Certificados digitais A3, na nuvem, pessoa física	40 unidades	36 meses para cada certificado, e 36 meses de contrato, renovável por mais 36 meses.

7.2. A quantidade foi definida com base nas necessidades atuais das unidades administrativas e técnicas, podendo atender novos servidores e substituições por vencimento dos certificados vigentes.

8. Levantamento de soluções

8.1. O levantamento de soluções visa identificar e comparar alternativas disponíveis no mercado que possam atender às necessidades do JBRJ.

8.1.1. Solução 1: Certificado A1 (arquivo eletrônico) – armazenado no computador.

8.1.2. Solução 2: Certificado A3 com cartão e leitora – exige aquisição de cartão físico e leitora específica.

8.1.3. Solução 3: Certificado A3 com token USB – solução compacta, segura e de fácil transporte.

8.1.4. Solução 4: Certificado A3, na nuvem – solução compacta, segura e de fácil transporte.

9. Análise comparativa de soluções

9.1. Durante o levantamento de soluções disponíveis no mercado, foram identificadas três principais alternativas para atender à necessidade do JBRJ, conforme descrito a seguir:

9.1.1. Solução 1: Certificado A1 (arquivo eletrônico) – Certificado emitido e armazenado diretamente em um computador, sendo protegido por senha. Possui validade de até 12 meses e não requer dispositivos físicos adicionais.

9.1.2. Vantagens:

9.1.2.1. Custo unitário reduzido em comparação ao A3.

9.1.2.2. Instalação e emissão mais ágeis.

9.1.2.3. Não requer dispositivos físicos (token ou cartão).

9.1.3. Desvantagens:

9.1.3.1. Menor nível de segurança, pois o certificado fica armazenado localmente.

9.1.3.2. Maior vulnerabilidade a perda, roubo de dados ou uso indevido.

9.1.3.3. Necessidade de renovação anual, aumentando custos administrativos a médio prazo.

9.1.3.4. Impossibilidade de uso em diferentes estações de trabalho sem exportação do arquivo, o que aumenta riscos de segurança.

9.1.4. Solução 2: Certificado A3 com cartão e leitora – Certificado armazenado em cartão inteligente, acessado por meio de leitora específica conectada ao computador.

9.1.5. Vantagens:

9.1.5.1. Elevado nível de segurança, pois o armazenamento é físico e criptografado.

9.1.5.2. Impossibilidade de cópia ou clonagem do certificado.

9.1.5.3. Maior controle de uso, sendo exigida autenticação física para cada operação.

9.1.6. Desvantagens:

9.1.6.1. Necessidade de aquisição e configuração de leitora específica, aumentando custos.

9.1.6.2. Menor praticidade no transporte e uso, especialmente em ambientes de trabalho com estações compartilhadas.

9.1.6.3. Maior tempo de instalação e suporte técnico.

9.1.6.4. Custo total superior ao certificado A3 com token.

9.1.7. Solução 3: Certificado A3 com token USB – Certificado armazenado em dispositivo criptográfico portátil (token USB), dispensando leitora externa.

9.1.8. Vantagens:

9.1.8.1. Alto nível de segurança, com proteção contra cópia e uso não autorizado.

9.1.8.2. Facilidade de transporte e uso em diferentes estações de trabalho.

9.1.8.3. Emissão com validade de até 36 meses, reduzindo custos de renovação.

9.1.8.4. Não requer periféricos adicionais (como leitora), reduzindo custos e complexidade.

9.1.8.5. Compatível com os principais sistemas operacionais utilizados no órgão (Windows, Linux e macOS).

9.1.9. Desvantagens:

9.1.9.1. Custo inicial ligeiramente superior ao certificado A1.

9.1.9.2. Exige manuseio físico do dispositivo, o que requer cuidados para evitar perda ou dano.

9.1.10. Solução 4: Certificado A3, na nuvem.

9.1.11. Vantagens:

9.1.11.1. Maior praticidade e mobilidade - Permite a realização de assinaturas digitais em celular, sem necessidade de portar token físico.

9.1.11.2. Redução do risco de extravio ou dano físico - Elimina a dependência de dispositivo criptográfico (token USB), evitando problemas decorrentes de perda, quebra ou incompatibilidade do hardware.

9.1.11.3. Facilidade operacional - Dispensa instalação de drivers específicos e reduz chamados técnicos relacionados a falhas de leitura ou reconhecimento de token.

9.1.11.4. Segurança reforçada **-** Utiliza autenticação em dois fatores (senha + validação no celular), com armazenamento da chave privada em ambiente seguro e certificado, reduzindo riscos de cópia indevida da chave.

9.1.11.5. Continuidade do serviço **-** Em caso de troca de computador, não há necessidade de reinstalação física do certificado, bastando autenticação no sistema.

9.1.12. Desvantagens:

9.1.12.1. Dependência de dispositivo móvel **-** Requer celular compatível para autenticação das assinaturas, o que pode demandar configuração inicial e suporte ao usuário.

9.2. Considerando os aspectos de segurança, mobilidade, redução de riscos operacionais e alinhamento às orientações para contratação junto a Autoridade Certificadora de Governo, a solução de Certificado Digital A3 em nuvem, pessoa física, e Certificado A3 com token USB, pessoa física, mostra-se tecnicamente adequada e mais vantajosa em comparação à alternativa com token físico, certificado A1, e certificado A3 com cartão e leitora, especialmente no contexto de uso institucional e necessidade de praticidade operacional.

10. Registro de soluções consideradas inviáveis

10.1. Conforme item 9, a solução considerada inviável é a solução 1, certificado A1 (arquivo eletrônico), inviável devido ao armazenamento local, que aumenta o risco de perda ou uso indevido, e solução 2, cartão com leitora, solução mais onerosa, com maior complexidade de uso e necessidade de periféricos adicionais.

11. Análise comparativa de custos (TCO)

11.1. Para calcular o preço unitário de referência, solicitamos cotações a fornecedores especializados no ramo, conforme tabela abaixo:

Certificado A1 (arquivo eletrônico)

Especificação	**Unid Medida**	**Quant.**	**Banco de preços**	**Média 12 meses**
Certificado A1 (arquivo eletrônico). **Período de 12 meses.**	Un	60	R$120,00	**R$7.200,00**

Certificado A3 com cartão e leitora

Especificação	Unid Medida	Quant.	Banco de preços	Média 12 meses
Certificado A3 com cartão e leitora. **Período de 12 meses.**	Un	60	R$320,00	**R$19.200,00**

Certificado A3 com token USB

Especificação	Unid Medida	Quant.	Comercial Certising	Ar Digital Rio Certificados	Média 72 meses
Certificação Digital A3, do tipo pessoa física (e-CPF), com dispositivos de Token USB. **Período de 36 meses para cada dispositivo.**	Un	60	R$412,40	R$310,00	**R$21.672,00**

Certificado A3 com token USB Serpro

Especificação	Unid Med.	Quant.	Serpro	Média 72 meses
Certificação Digital A3, do tipo pessoa física (e-CPF), com dispositivos de Token USB. **Período de 36 meses para cada dispositivo.**	Un	60	R$241,16	**R$14.469,60**

Certificado A3 nuvem Serpro

Especificação	Unid Medida	Quant.	Serpro/ Nuvem	Média 72 meses
Certificação Digital A3, do tipo pessoa física (e-CPF), na nuvem.				

Período de 36 meses para cada dispositivo.	Un	60	R$179,90	**R$ 10.168,20**

11.2. Foi utilizada a plataforma de preços de contratações públicas similares, em órgãos do âmbito federal, Banco de Preços, levando em consideração a média e o menor dos valores obtidos.

11.3. Para realização desta demanda realizamos pesquisa de preço para:

11.3.1. Certificado A1 (arquivo eletrônico);

11.3.2. Certificado A3 com cartão e leitora; e

11.3.3. Certificado A3 com token USB.

11.4. Para Certificado A1 (arquivo eletrônico), utilizamos o sistema banco de preços.

11.5. Para Certificado A3 com cartão e leitora, utilizamos o sistema banco de preços.

11.6. Para Certificado A3 com token USB**,** utilizamos cotações com empresas privadas.

11.7. Em adição, realizamos consulta direta com fornecedores do ramo, como Local Bussiness e Online Certificadora, no entanto, nenhuma das empresas nos retornou, conforme registrado nas mensagens eletrônicas anexadas ao processo.

11.8. Por fim, solicitamos proposta a empresa Serpro, que nos enviou duas propostas:

11.8.1. Certificado A3 com token USB; e;

11.8.2. Certificado A3 nuvem.

11.9. Em razão das alterações nos requisitos de acesso ao SIAFI, os certificados digitais a serem contratados devem estar em conformidade com as orientações estabelecidas pela Secretaria do Tesouro Nacional, conforme diretrizes disponíveis em: https://www.gov.br/tesouronacional/pt-br/siafi/como-acessar/mudancas_acesso-siafi. Nesse contexto, destaca-se a exigência de que os certificados digitais sejam emitidos por Autoridades Certificadoras de Governo, de modo a atender aos requisitos de segurança e autenticação estabelecidos para o acesso ao sistema.

11.20. Diante dessas exigências, a aquisição de certificados digitais do tipo A3, na modalidade em nuvem, para pessoa física, e certificado A3 com token USB, apresenta-se como a alternativa mais vantajosa para a Administração Pública, considerando aspectos de segurança, custo-benefício e durabilidade da solução. Tais certificados possuem validade de 36 (trinta e seis) meses, com possibilidade de renovação por igual período, o que contribui para a redução da frequência de novas contratações em curto prazo e, consequentemente, para a diminuição dos custos administrativos associados ao processo de aquisição.

11.21. Em contraste, os Certificados Digitais do tipo A1 (arquivo eletrônico) e o A3 com cartão e leitora possuem validade de apenas 12 (doze) meses, demandando renovações anuais e maior esforço administrativo para sua gestão. Ademais, tais soluções não atendem às alterações nos requisitos de acesso ao SIAFI, conforme orientações estabelecidas pela Secretaria do Tesouro Nacional para utilização de certificados emitidos por Autoridades Certificadoras de Governo.

12. Descrição da solução de TIC a ser contratada

12.1. Contratação de 40 (quarenta) certificados digitais A3, na nuvem, pessoa física, e 20 (vinte) certificados Digitais A3 – e - CPF, com dispositivo Token USB, emitidos por autoridades certificadoras de governo, com validade de 36 meses, para cada certificado e token, 36 meses de contrato, renovável por mais 36 meses, incluindo suporte técnico para emissão, instalação e ativação dos certificados e tokens.

13. Estimativa de custo total da contratação

Valor (R$): 11.602,00

13.1. O custo estimado total da contratação é de **R$11.602,00** (onze mil seiscentos e dois reais).

14. Justificativa técnica da escolha da solução

14.1. Considerando os aspectos de segurança, mobilidade, redução de riscos operacionais e alinhamento às orientações para contratação junto a Autoridade Certificadora de Governo, a solução 3 Certificado A3 com token USB, e solução 4, de Certificado Digital A3 em nuvem mostra-se tecnicamente adequada e mais vantajosa em comparação aos outros, especialmente no contexto de uso institucional e necessidade de praticidade operacional.

14.2. Em contraste, os Certificados Digitais do tipo A1 (arquivo eletrônico) e o A3 com cartão e leitora possuem validade de apenas 12 (doze) meses, demandando renovações anuais e maior esforço administrativo para sua gestão. Ademais, tais soluções não atendem às alterações nos requisitos de acesso ao SIAFI, conforme orientações estabelecidas pela Secretaria do Tesouro Nacional para utilização de certificados emitidos por Autoridades Certificadoras de Governo.

15. Justificativa econômica da escolha da solução

15.1. A contratação representa ótima relação custo-benefício, visto que o valor unitário do certificado digital A3 em nuvem, e certificado Digitais A3 – e-CPF, com dispositivo Token USB é competitivo.

15.2. Além disso, a validade de 36 meses para cada certificado, e 36 meses de contrato, renovável por mais 36 meses, reduz a necessidade de renovações frequentes, gerando economia administrativa e financeira ao órgão.

15.3. Diante dessas exigências, a aquisição de certificados digitais do tipo A3, na modalidade em nuvem, para pessoa física, e e certificado Digitais A3 – e-CPF, com dispositivo Token USB, apresenta-se como a alternativa mais vantajosa para a Administração Pública, considerando aspectos de segurança, custo-benefício e durabilidade da solução.

16. Benefícios a serem alcançados com a contratação

16.1. Aumento da segurança nas transações e assinaturas eletrônicas;

16.2. Agilidade na tramitação de processos e documentos oficiais;

16.3. Redução de custos operacionais e de impressão de documentos;

16.4. Modernização e eficiência administrativa no âmbito do JBRJ;

16.5.Contribuição para a sustentabilidade, por meio da redução do uso de papel e transporte de documentos físicos.

17. Providências a serem Adotadas

17.1. Após a realização desse Estudo Técnico Preliminar, o Termo de Referência será elaborado e caso aprovado pela Administração Central será realizada a melhor escolha para a contratação dos serviços em tela.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Diante da análise apresentada neste Estudo Técnico Preliminar, a equipe de planejamento manifesta-se favoravelmente à viabilidade da contratação.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

CHRISTIAN BRENO WANDERMUREM VILELA

Integrante técnico

Assinou eletronicamente em 22/04/2026 às 12:18:13.

BRUNO AUGUSTO DE FARIAS

Integrante Requisitante

Assinou eletronicamente em 22/04/2026 às 11:50:44.

FABIO ARNALDO DE SOUZA AGUIAR MIRANDA

Integrante administrativo

Assinou eletronicamente em 22/04/2026 às 11:55:55.

WELINGTON RODRIGUES BRAGA

Coordenador de TI

Assinou eletronicamente em 22/04/2026 às 12:02:08.