

DEFENSORIA PUBLICA DA UNIAO

Estudo Técnico Preliminar 30/2026**1. Informações Básicas**

Número do processo: 08038.000579/2026-32

2. Descrição da necessidade

2.1. A Defensoria Pública da União – DPU depende do uso de certificados digitais no padrão ICP-Brasil para assegurar a validade jurídica dos atos praticados eletronicamente, garantindo autenticidade, integridade, confidencialidade e não repúdio em atividades institucionais essenciais, tais como:

- assinatura de documentos administrativos e judiciais;
- autenticação segura em sistemas governamentais;
- acesso a plataformas institucionais e estruturantes;
- execução de operações eletrônicas de elevada criticidade institucional.

2.2. Atualmente, a DPU mantém contratação com o Serviço Federal de Processamento de Dados – SERPRO para fornecimento da solução de certificação digital em nuvem NeoID, cujo contrato vigente possui término previsto para 14/04/2026, tornando necessária a realização de nova contratação a fim de assegurar a continuidade operacional dos serviços institucionais dependentes da certificação digital.

2.3. A solução NeoID representa evolução tecnológica em relação ao modelo tradicional baseado em certificados A3 armazenados em mídias físicas (tokens ou cartões), pois:

- elimina a necessidade de dispositivos criptográficos físicos;
- reduz custos logísticos e operacionais de suporte;
- possibilita gestão centralizada de identidades digitais;
- melhora a experiência do usuário;
- amplia a mobilidade e disponibilidade do serviço.

2.4. Do ponto de vista técnico, as chaves criptográficas são armazenadas em ambiente seguro baseado em Hardware Security Module (HSM), com autenticação forte e integração nativa às plataformas governamentais digitais.

2.5. A eventual interrupção do serviço de certificação digital acarretaria impactos diretos nas atividades finalísticas e administrativas da DPU, especialmente quanto:

- à assinatura eletrônica de documentos;
- ao acesso seguro a sistemas estruturantes;
- à tramitação processual eletrônica;
- ao cumprimento de prazos legais e institucionais,

2.5.1. Podendo resultar na paralisação parcial de atividades essenciais e prejuízo à prestação do serviço público.

2.6. Considerando que o Serviço Federal de Processamento de Dados – SERPRO é empresa pública federal especializada na prestação de serviços de tecnologia da informação à Administração Pública, detentora da solução governamental NeoID, a contratação mostra-se adequada mediante contratação direta, com fundamento no art. 75, inciso IX, da Lei nº 14.133/2021, observados os princípios da eficiência, continuidade do serviço público e vantajosidade administrativa.

3. Área requisitante

| Área Requisitante | Responsável |
|---------------------------------------|---------------------------------------|
| Secretaria de Gestão de Pessoas - SGP | Joelma Maria de Sousa Bezerra Feitosa |

4. Necessidades de Negócio

4.1. A Defensoria Pública da União (DPU) depende da utilização de certificados digitais no padrão ICP-Brasil para assegurar a validade jurídica, autenticidade, integridade e o não repúdio dos atos administrativos e judiciais praticados eletronicamente por seus membros e servidores. Esses certificados constituem elemento essencial para a execução das atividades institucionais, viabilizando a assinatura digital de documentos oficiais, a autenticação segura em sistemas governamentais e a realização de operações que exigem identificação digital confiável.

4.2. A certificação digital sustenta o funcionamento cotidiano da instituição, uma vez que diversos sistemas estruturantes da Administração Pública exigem autenticação baseada em certificado digital do tipo A3, tais como SEI, PJe/e-Proc, SIAFI, SIGEPE, Compras.gov.br, e-CAC e demais plataformas de governo eletrônico utilizadas pela DPU. Dessa forma, a disponibilidade contínua desse serviço configura requisito operacional indispensável ao desempenho das atribuições institucionais.

4.3. A ampliação do uso de processos eletrônicos e a adoção de modelos de trabalho remoto e híbrido intensificaram a dependência institucional de mecanismos de autenticação digital segura. Nesse contexto, membros e servidores necessitam acessar sistemas, assinar documentos e praticar atos administrativos e processuais independentemente de sua localização física, exigindo solução que ofereça mobilidade, disponibilidade e segurança compatíveis com as demandas institucionais.

4.4. A eventual interrupção do serviço de certificação digital impactaria diretamente processos críticos da organização, incluindo:

- I – assinatura de atos administrativos e judiciais;
- II – autenticação em sistemas estruturantes do Governo Federal;
- III – execução de operações financeiras e fiscais;
- IV – instrução e tramitação de processos internos;
- V – comunicações institucionais oficiais; e
- VI – validação de atos sujeitos a controle, auditoria e fiscalização.

4.5. A indisponibilidade desses serviços pode ocasionar paralisação de atividades essenciais, descumprimento de prazos legais, riscos operacionais e jurídicos, além de prejuízos à prestação do serviço público e ao atendimento ao cidadão.

4.6. A adoção da certificação digital em nuvem representa evolução tecnológica em relação ao modelo baseado em dispositivos físicos, ao eliminar dependências logísticas, reduzir custos operacionais associados à gestão de mídias criptográficas e ampliar a experiência do usuário, promovendo maior eficiência administrativa e aderência às diretrizes de transformação digital da Administração Pública Federal.

4.7. Assim, a necessidade de negócio consiste em assegurar solução de certificação digital institucional que garanta continuidade operacional, segurança da informação, mobilidade dos usuários e integração adequada ao ecossistema de serviços digitais governamentais, sustentando a execução regular das atividades finalísticas e administrativas da DPU.

5. Necessidades Tecnológicas

5.1. A contratação do serviço de certificação digital em nuvem NeoID, fornecido pelo Serviço Federal de Processamento de Dados – SERPRO, deve atender a um conjunto de necessidades tecnológicas essenciais à garantia de segurança da informação, disponibilidade operacional, interoperabilidade sistêmica e eficiência administrativa nos processos eletrônicos da Defensoria Pública da União (DPU).

5.2. Tais necessidades decorrem da crescente digitalização das atividades institucionais e da dependência de mecanismos confiáveis de identificação digital, sendo indispensáveis para assegurar a continuidade da transformação digital do órgão, mitigar riscos operacionais e garantir conformidade com normas nacionais de segurança e certificação digital.

5.3. Nesse contexto, a solução contratada deverá contemplar, no mínimo, os seguintes requisitos tecnológicos:

5.3.1. Segurança criptográfica

- a) geração, armazenamento e proteção das chaves criptográficas em Hardware Security Module (HSM) certificado;**
- b) impossibilidade de exportação das chaves privadas;**
- c) mecanismos de controle de acesso, segregação de funções e proteção contra uso indevido.**

5.3.2. Autenticação forte

- a) suporte a autenticação multifator (MFA);**
- b) utilização de múltiplos fatores de verificação, como senha, biometria ou mecanismos equivalentes;**
- c) compatibilidade com os padrões de autenticação adotados pelo Governo Federal.**

5.3.3. Integração com o ecossistema governamental

- a) interoperabilidade com sistemas estruturantes da Administração Pública Federal;**
- b) compatibilidade com plataformas como gov.br, SIGEPE e demais barramentos e APIs governamentais;**
- c) integração transparente com sistemas institucionais utilizados pela DPU.**

5.3.4. Conformidade normativa

- a) aderência integral às normas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil;**
- b) conformidade com a Lei nº 13.709/2018 (LGPD);**
- c) observância das políticas institucionais de segurança da informação e boas práticas de auditoria.**

5.3.5. Disponibilidade e continuidade do serviço

- a) operação contínua do serviço, com disponibilidade compatível à criticidade institucional;**
- b) mecanismos de redundância e alta disponibilidade;**
- c) existência de Plano de Continuidade de Negócios (BCP) e Recuperação de Desastres (DR), com objetivos de recuperação (RTO) e perda aceitável de dados (RPO) compatíveis com serviços críticos.**

5.3.6. Escalabilidade

- a) capacidade de expansão do serviço conforme crescimento da demanda institucional;**
- b) manutenção do desempenho mesmo em períodos de pico de utilização.**

5.3.7. Auditabilidade e rastreabilidade

- a) registro de trilhas de auditoria das operações realizadas;**
- b) disponibilização de logs de autenticação e assinatura digital;**
- c) possibilidade de exportação dos registros para fins de controle interno, auditoria e conformidade.**

5.3.8. Simplicidade operacional

- a) eliminação da dependência de mídias físicas (tokens ou cartões);**
- b) dispensa de instalação de drivers locais;**
- c) redução da carga operacional de suporte técnico e gestão de ativos criptográficos.**

5.4. O atendimento a esses requisitos tecnológicos é condição necessária para garantir que a solução contratada sustente, de forma segura e contínua, as operações digitais da DPU, assegurando eficiência administrativa, conformidade regulatória e confiabilidade

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

6.1. A escolha da solução de certificação digital em nuvem NeoID, prestada pelo Serviço Federal de Processamento de Dados — SERPRO, deve observar um conjunto de requisitos adicionais que justificam e fundamentam técnica e institucionalmente a seleção dessa alternativa como a mais adequada para atender às necessidades da Defensoria Pública da União (DPU).

6.2. Esses requisitos complementam as necessidades de negócio e tecnológicas já identificadas, assegurando que a solução atenda plenamente aos objetivos estratégicos, legais, operacionais e de segurança da informação do órgão.

6.3. Continuidade e maturidade da solução

6.3.1. A solução encontra-se previamente implantada e em operação no ambiente institucional da DPU, apresentando resultados satisfatórios quanto à estabilidade, segurança e desempenho, o que reduz riscos de transição tecnológica, descontinuidade operacional e necessidade de novos ciclos de adaptação dos usuários.

6.4. Exclusividade da solução

6.4.1. A contratação fundamenta-se na condição de fornecedor integrante da Administração Pública responsável pela disponibilização da solução NeoID, desenvolvida e operada pelo Serviço Federal de Processamento de Dados (SERPRO), cuja arquitetura tecnológica, modelo operacional e integração nativa com plataformas governamentais federais não possuem equivalência funcional no mercado.

6.4.2. A pesquisa de mercado realizada evidenciou que, embora existam certificados digitais padrão ICP-Brasil ofertados por diversas Autoridades Certificadoras, nenhuma alternativa apresenta o mesmo nível de integração governamental, gestão centralizada, interoperabilidade institucional e aderência às infraestruturas digitais da Administração Pública Federal.

6.4.3. Assim, a escolha da solução decorre da sua adequação técnica e institucional às necessidades do órgão, caracterizando hipótese de contratação direta com fundamento no art. 75, inciso IX, da Lei nº 14.133/2021, não em razão de inviabilidade absoluta de competição, mas pela natureza pública do fornecedor e pela especificidade da solução disponibilizada no âmbito da Administração Pública.

6.5. Aderência às diretrizes de Governo Digital

6.5.1. A solução deve manter compatibilidade com as políticas e diretrizes de transformação digital da Administração Pública Federal, especialmente no que se refere à identidade digital governamental, autenticação segura e interoperabilidade entre sistemas públicos.

6.6. Interoperabilidade sistêmica

6.6.1. A solução deverá operar de forma integrada com sistemas institucionais internos e plataformas externas da Administração Pública, garantindo interoperabilidade tecnológica e continuidade dos fluxos eletrônicos de trabalho.

6.7. Economicidade operacional

6.7.1. O modelo de certificação em nuvem deverá proporcionar redução de custos operacionais indiretos, especialmente aqueles relacionados à aquisição, logística, manutenção e suporte de mídias criptográficas físicas, além da diminuição da demanda por atendimento técnico especializado.

6.8. Escalabilidade e facilidade operacional

6.8.1. A solução deverá permitir expansão gradual do quantitativo de certificados digitais conforme a evolução das necessidades institucionais, sem impacto relevante na infraestrutura tecnológica ou aumento significativo da complexidade operacional, assegurando rápida adoção pelos usuários e menor curva de aprendizado.

6.9. O conjunto de requisitos acima apresentados demonstra que a solução NeoID, fornecida pelo SERPRO, atende de forma completa aos critérios de continuidade operacional, segurança, economicidade, interoperabilidade e alinhamento às políticas

governamentais, constituindo alternativa tecnicamente adequada e suficiente para fundamentar a escolha da solução e a contratação por continuidade, garantindo estabilidade operacional e evolução tecnológica na gestão da identidade digital institucional da DPU.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A Defensoria Pública da União (DPU) estima a contratação de 1.034 (mil e trinta e quatro) certificados digitais do tipo NeoID, já contemplando reserva técnica de 10% (dez por cento) aplicada sobre o quantitativo anual projetado, conforme parâmetros definidos na Nota Técnica da Coordenação de Gerenciamento do Cadastro e Registro Funcionais (SEI nº 8736793).

7.2. Além dos certificados NeoID, está prevista a aquisição de outros tipos de certificados digitais, totalizando 1.784 (mil setecentos e oitenta e quatro) certificados, considerando a consolidação da demanda institucional atual e a previsão de crescimento orgânico do uso de identidade digital no âmbito da DPU.

7.3. O valor global apresentado pelo Serviço Federal de Processamento de Dados – SERPRO para o fornecimento do conjunto de 1.784 certificados digitais corresponde a R\$ 149.784,78 (cento e quarenta e nove mil, setecentos e oitenta e quatro reais e setenta e oito centavos).

7.4. Considerando o período contratual estimado de 60 (sessenta) meses, o valor global representa aproximadamente:

- R\$ 29.956,96 (vinte e nove mil, novecentos e cinquenta e seis reais e noventa e seis centavos) por ano; e
- R\$ 2.496,41 (dois mil, quatrocentos e noventa e seis reais e quarenta e um centavos) por mês, em valores proporcionais.

7.5. Por se tratar de contratação direta por dispensa de licitação, nos termos do art. 75, inciso IX, da Lei nº 14.133/2021, a estimativa de preços foi realizada com base na análise de contratações similares celebradas por outros órgãos da Administração Pública Federal, cujos instrumentos e documentos comprobatórios foram juntados aos autos, permitindo a verificação da compatibilidade dos valores praticados e a aferição da razoabilidade econômica da contratação pretendida.

7.5.1. A análise comparativa demonstrou que os preços apresentados encontram-se alinhados aos valores praticados pela Administração Pública em contratações de objeto equivalente, evidenciando a adequação econômica da solução e observando os princípios da economicidade, eficiência e vantajosidade administrativa.

7.5.2. Dessa forma, considera-se atendido o requisito de justificativa de preços exigido para contratações diretas, restando demonstrada a compatibilidade da proposta com os parâmetros de mercado e com as práticas adotadas pela Administração Pública Federal.

7.6. Tabela Resumo:

| ITEM | QUANTITATIVO | OBSERVAÇÃO |
|------------------------------|----------------|-------------------------------|
| Certificados NeoID | 1.034 | Inclui reserva técnica de 10% |
| Demais certificados digitais | 750 | Complementares ao NeoID |
| Total de certificados | 1.784 | Consolidado (NeoID + demais) |
| Valor global (5 anos) | R\$ 149.784,78 | Proposta SERPRO |
| Valor anual aproximado | R\$ 29.956,96 | Distribuição proporcional |

| | | |
|-------------------------|--------------|---------------------------|
| Valor mensal aproximado | R\$ 2.496,41 | Distribuição proporcional |
|-------------------------|--------------|---------------------------|

8. Levantamento de soluções

8.1. Soluções disponíveis no mercado

8.1.1. Durante o levantamento técnico, foram identificadas as principais categorias de soluções de certificação digital atualmente disponíveis no mercado brasileiro, dentre as quais destacam-se:

8.1.1.1. Certificados digitais padrão ICP-Brasil (A1/A3)

8.1.1.1.1. São emitidos por diversas Autoridades Certificadoras (AC), tais como:

- Valid
- Soluti
- Serasa Experian
- Certisign
- Caixa Econômica Federal
- Correios, entre outras.

8.1.1.2. Esses certificados possuem ampla utilização no país e seguem o modelo da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), permitindo autenticação, assinatura digital e garantia de integridade de documentos eletrônicos.

8.1.1.3. Limitações para o caso em análise

8.1.1.3.1. Embora atendam aos requisitos gerais da ICP-Brasil, tais soluções:

- não possuem integração nativa com os sistemas governamentais utilizados pela DPU;
- não oferecem modelo centralizado de gestão institucional de identidades digitais compatível com o ecossistema federal;
- demandariam customizações, integrações adicionais e adaptações operacionais, com aumento de custo, risco técnico e prazo de implantação.

8.1.1.4. Assim, não atendem de forma imediata às necessidades institucionais já suportadas pela solução atualmente utilizada.

8.2. Soluções privadas de identidade digital não certificadas pela ICP-Brasil

8.2.1. O mercado também disponibiliza soluções privadas de autenticação digital, tais como:

- plataformas de Identity and Access Management (IAM);
- soluções de login federado/social (Google, Microsoft, entre outras);
- serviços de verificação e onboarding digital com biometria.

8.2.2. Limitações para o caso em análise

8.2.2.1. Essas soluções apresentam restrições relevantes:

- não possuem certificação ICP-Brasil;
- não asseguram validade jurídica equivalente à assinatura digital qualificada;
- não atendem aos requisitos legais exigidos para atos administrativos e judiciais;
- não apresentam aderência aos padrões de integração do ecossistema governamental federal.

8.2.2.2. Dessa forma, não se mostram aptas ao atendimento das necessidades institucionais da DPU.

8.3. Soluções de identidade digital governamental de outros órgãos

8.3.1. Foram consideradas iniciativas públicas existentes, tais como:

- Login único GOV.BR;
- certificados institucionais emitidos internamente por determinados órgãos para uso restrito.

8.3.2. Limitações para o caso em análise

8.3.2.1. Tais soluções possuem escopo distinto e não substituem certificados digitais ICP-Brasil utilizados para:

- assinatura eletrônica qualificada;
- autenticação em sistemas estruturantes;
- operações institucionais com validade jurídica plena.

8.4. Solução NeoID do SERPRO

8.4.1. O NeoID constitui solução de certificação digital em nuvem desenvolvida pelo Serviço Federal de Processamento de Dados – SERPRO, empresa pública federal responsável por soluções tecnológicas estruturantes da Administração Pública. A solução apresenta as seguintes características:

8.4.1.1. integração nativa com barramentos, APIs e plataformas governamentais federais;

8.4.1.2. gestão centralizada de identidades digitais institucionais;

8.4.1.3. arquitetura tecnológica própria voltada ao ambiente governamental;

8.4.1.4. mecanismos de segurança compatíveis com padrões federais de proteção da informação;

8.4.1.5. suporte especializado para sistemas estruturantes da Administração Pública.

8.5. Justificativa da escolha da solução

8.5.1. O levantamento de mercado demonstrou que existem alternativas privadas de certificação digital; entretanto, tais soluções não apresentam o mesmo nível de integração operacional, governança institucional e aderência ao ecossistema tecnológico do Governo Federal requerido pela DPU.

8.5.2. A contratação do NeoID fundamenta-se:

- na continuidade da solução já implantada e operacional;
- na aderência às políticas de Governo Digital;
- na integração direta com sistemas federais;
- na redução de riscos operacionais e custos de transição.

8.6. Assim, a contratação enquadra-se na hipótese de dispensa de licitação prevista no art. 75, inciso IX, da Lei nº 14.133/2021, por tratar-se de contratação realizada com empresa pública integrante da Administração Pública Federal, criada para prestar serviços tecnológicos especializados à própria Administração, mostrando-se a solução mais adequada ao atendimento do interesse público.

9. Análise comparativa de soluções

9.1. O quadro comparativo a seguir apresenta a análise das soluções identificadas no levantamento de mercado, avaliando sua capacidade de atendimento às necessidades de negócio, tecnológicas e institucionais da Defensoria Pública da União (DPU).

9.2. As alternativas foram examinadas considerando critérios técnicos, operacionais, legais e de integração governamental, especialmente quanto à aderência aos requisitos de certificação digital ICP-Brasil, interoperabilidade com sistemas estruturantes da Administração Pública Federal e viabilidade de implementação no ambiente institucional da DPU.

| Requisito | Outras Soluções | Certificado NeoID SERPRO |
|---|------------------------|---------------------------------|
| 1. Modernização Tecnológica | Atende | Atende |
| 2. Tempestividade no atendimento de necessidades | Não Atende | Atende |
| 3. Integração de Sistemas | Não Atende | Atende |
| 4. Melhoria da Eficiência Operacional | Não Atende | Atende |
| 5. Aprimoramento da Transparência e Prestação de Contas | Atende | Atende |
| 6. Cumprimento de Requisitos Legais e Regulatórios | Atende | Atende |
| 7. Melhoria da Experiência do Usuário | Atende | Atende |
| 8. Suporte a Programas e Projetos Estratégicos | Atende | Atende |
| 9. Preservação dos sistemas integrados à nuvem | Atende | Atende |
| 10. Acesso ao catálogo completo de serviços multinuvm | Parcialmente | Atende |
| 11. Atualização dos ativos de TI da DPU | Atende | Atende |
| 12. Saneamento das vulnerabilidades de TIC | Atende | Atende |
| 13. Automação de processos de gestão de TIC | Atende | Atende |
| 14. Flexibilidade | Parcialmente | Atende |
| 15. Não onerosidade | Não atende | Atende |
| 16. Plurianualidade | Atende | Atende |
| 17. Variedade | Atende | Atende |
| 18. Padronização | Atende | Atende |
| 19. Não duplicidade de objetos | Atende | Atende |
| | | |

9.3. Além da solução adotada, foram consideradas alternativas disponíveis no mercado, especialmente certificados digitais no padrão ICPBrasil ofertados por Autoridades Certificadoras privadas.

9.4. Todavia, tais soluções mostraram-se inadequadas ao contexto da Administração Pública Federal, por não oferecerem integração nativa com plataformas governamentais estruturantes, não possibilitarem gestão centralizada de identidades digitais institucionais e não apresentarem aderência plena às políticas federais de segurança da informação, computação em nuvem e governança de dados.

9.5. Ademais, a adoção dessas alternativas demandaria adaptações técnicas, desenvolvimento adicional e investimentos complementares, com impactos negativos à continuidade do serviço, à segurança da informação e à eficiência operacional.

9.6. Assim, sob os aspectos técnico, operacional e de governança, concluiu-se que tais soluções não atendem de forma equivalente aos requisitos da contratação, reforçando a adequação da solução NeoID.

10. Registro de soluções consideradas inviáveis

10.1. Durante o levantamento de mercado e análise das alternativas tecnológicas, foram identificadas soluções que, embora semelhantes ao tema de certificação digital, mostraram-se inviáveis para o atendimento das necessidades específicas da DPU. A rejeição das soluções ofertadas por Autoridades Certificadoras (AC) privadas (como Certisign, Serasa Experian, Valid, Soluti, entre outras) fundamenta-se nos seguintes critérios técnicos e operacionais:

10.1.1. Inexistência de Integração Nativa com o Ecossistema Federal: As soluções privadas não possuem integração nativa com os barramentos governamentais, APIs e Gateways do Governo Federal (como o API Gateway Gov e barramentos do SERPRO), o que exigiria desenvolvimentos adicionais complexos, custos de customização e elevaria o tempo de implementação.

10.1.2. Ausência de Gestão Centralizada Federada: Diferente do NeoID, as alternativas de mercado não oferecem mecanismos de gestão centralizada de identidades que permitam a autenticação federada específica para as plataformas estruturantes utilizadas pela DPU, tais como SEI, PJe, e-Proc, SIAFI e SIGEPE.

10.1.3. Incompatibilidade com Requisitos de Soberania e Segurança Estatal: As soluções privadas foram consideradas inadequadas por não apresentarem aderência plena às políticas federais de segurança da informação e soberania de dados, especialmente no que tange ao armazenamento de chaves em Hardware Security Module (HSM) com integração direta às infraestruturas de autenticação pública do SERPRO.

10.2. Soluções de Identidade Digital de Outros Órgãos Iniciativas como o login único do GOV.BR e certificados de uso restrito de outros órgãos foram descartadas por possuírem escopo limitado, não ofertando o conjunto de características técnicas, arquitetura de autenticação e suporte direto aos fluxos avançados de assinatura exigidos para a sustentação dos atos processuais e administrativos da Defensoria.

10.3. Gerenciamento do Risco de Dependência Tecnológica (Vendor Lock-in), para mitigar o risco de dependência tecnológica (aprisionamento tecnológico) e garantir a reversibilidade do serviço, a modelagem da contratação estabelece os seguintes mecanismos:

10.3.1. Portabilidade e Reversibilidade: A solução NeoID permite a migração de dados e credenciais digitais ao término do contrato, garantindo que a DPU mantenha o controle sobre seu acervo de identidades.

10.3.2. Interoperabilidade ICP-Brasil: Por ser baseada no padrão aberto da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a solução garante que os atos assinados permaneçam válidos e verificáveis independentemente do fornecedor, facilitando a transição para outras Autoridades Certificadoras no futuro, se necessário.

10.3.3. Plano de Transição: O planejamento prevê a entrega de documentação operacional e suporte técnico da contratada durante o encerramento do vínculo, visando a transferência de conhecimento e o descarte seguro de dados de acordo com normas técnicas (NIST 800-88 ou equivalente).

10.4. Após análise detalhada, conclui-se que a solução NeoID do SERPRO é a única capaz de atender simultaneamente aos requisitos de negócio, segurança e interoperabilidade governamental. Tal constatação confirma a inviabilidade de competição com agentes privados e fundamenta tecnicamente a escolha da solução, assegurando a conformidade com o princípio da motivação e a eficiência administrativa.

10.5. Ao término do contrato, a Contratada deverá garantir a portabilidade dos dados e o histórico de emissões em formato interoperável, sem custos adicionais, assegurando que a DPU não sofra solução de continuidade ou dependência tecnológica impeditiva para migração de solução.

11. Análise comparativa de custos (TCO)

ANÁLISE DE CUSTO TOTAL (TCO – Total Cost of Ownership)

11.1. A análise de custo total considera não apenas o preço de aquisição do certificado digital, mas também os custos diretos, indiretos, operacionais e de manutenção ao longo da vida útil da solução, abrangendo impactos financeiros e administrativos decorrentes da sua utilização institucional.

11.2. Estudos técnicos públicos demonstram que certificados digitais do tipo A3 armazenados em token físico geram custos recorrentes relacionados à aquisição de hardware, reposição de dispositivos, suporte técnico especializado e logística de distribuição e recolhimento, além de riscos associados a extravio, danos físicos e incompatibilidades de drivers. Tais fatores acarretam elevado consumo de tempo e de recursos da área de Tecnologia da Informação para atendimento de incidentes e substituições.

11.3. Por sua vez, o certificado digital A3 em nuvem (NeoID) elimina a utilização de mídias físicas, reduzindo despesas relacionadas à aquisição e reposição de tokens, bem como diminuindo significativamente a necessidade de suporte técnico para instalação, atualização e manutenção de drivers. Experiências registradas em órgãos públicos indicam que a certificação digital em nuvem contribui para a redução da burocracia, simplificação operacional e diminuição dos custos administrativos.

11.4. Ademais, desde 2017, a Administração Pública Federal deixou de custear certificados digitais de forma centralizada, passando cada órgão a ser responsável pelo planejamento e custeio dessas soluções. Nesse cenário, alternativas que eliminam despesas com hardware e reduzem custos operacionais mostram-se mais vantajosas sob o aspecto econômico e gerencial.

11.5. Considerando o ciclo completo de validade típico dos certificados A3, verifica-se que a solução NeoID apresenta menor custo total de propriedade (TCO), menor volume de chamados de suporte técnico, maior disponibilidade operacional e elimina a necessidade de reposição de mídias físicas.

11.6. A tabela a seguir sintetiza as principais diferenças econômicas, operacionais e de manutenção entre as soluções analisadas.

| CRITÉRIO | CERTIFICADO A3 EM TOKEN (mídia física) | CERTIFICADO A3 EM NUVEM (NeoID – SERPRO) |
|---------------------|--|---|
| Custo de Aquisição | Alto: compra do token + certificado | Menor: apenas o certificado sem hardware |
| Custos recorrentes | Reposição de tokens, logística e suporte | Reduzidos: sem reposição física |
| Riscos operacionais | Extravio, danos, incompatibilidade de drivers | Mínimos: não há dispositivo físico |
| Suporte técnico | Alto: instalação, drivers e problemas de USB | Baixo: uso por app/portal, sem drivers |
| Mobilidade | Restrita ao uso do token e computador compatível | Alta: acessível em qualquer dispositivo conectado |

| | | |
|-----------------------------------|--|--|
| Produtividade | Limitada pelo uso presencial do token | Favorecida: ideal para trabalho híbrido/remoto |
| Disponibilidade | Depende da integridade do token | Alta: infraestrutura em nuvem redundante |
| Segurança | Chave no token físico | Chave em HSM certificado; maior proteção |
| Integração governamental | Compatível, porém dependente de configuração local | Integração nativa com gov.br e APIs do SERPRO |
| Auditabilidade | Limitada | Completa: logs e trilhas exportáveis |
| Gerenciamento | Descentralizado; depende da mídia física | Centralizado; gestão moderna e padronizada |
| Aderência à transformação digital | Baixa | Alta: elimina hardware e reduz burocracia |

11.7. Com base na análise realizada, verifica-se que:

11.7.1. Certificados armazenados em token físico apresentam custos totais mais elevados em razão da necessidade de aquisição de dispositivos, reposições frequentes e maior demanda operacional de suporte técnico.

11.7.2. O modelo NeoID, com certificado A3 armazenado em infraestrutura criptográfica em nuvem (HSM), reduz custos diretos e indiretos ao eliminar mídias físicas, simplificar o suporte técnico e reduzir demandas logísticas.

11.7.3. A solução em nuvem apresenta maior aderência às diretrizes de transformação digital da Administração Pública, favorecendo mobilidade, segurança e eficiência operacional.

11.7.4. Dessa forma, o custo total de propriedade do NeoID mostra-se mais vantajoso sob os aspectos econômico, operacional e tecnológico, atendendo de forma adequada às necessidades institucionais da Defensoria Pública da União.

11.8. Nos termos do inciso III do art. 11 da Instrução Normativa SGD/ME nº 94/2022, foi realizada análise comparativa do custo total de propriedade entre soluções tecnicamente viáveis. A avaliação demonstrou que a solução baseada em certificação digital em nuvem apresenta melhor relação custo-benefício e maior eficiência operacional, justificando sua adoção no âmbito da presente contratação direta, **com fundamento no art. 75, inciso IX, da Lei nº 14.133/2021.**

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

11.9. Para fins de obtenção, utilizamos como referência os valores unitários da Proposta de Preços encaminhada a DPU:

11.9.1. Ademais, O Índice de Custo da Tecnologia da Informação (ICTI), acumula uma variação de 6,4% nos últimos doze meses. Tal índice é aplicado ao valor estimado para as prorrogações subsequentes até o período de 36 (trinta e seis) meses.

TCO para contratação de serviços por 60 meses

| Descrição do Item | Quantidade Estimada (USN) | | Valor Total | |
|-------------------|---------------------------|----------|-------------|----------|
| | Mensal | 60 Meses | Mensal | 60 Meses |
| | | | | |

| | | | | |
|--|-------------|------|--------------|-----------------------|
| Contratação de certificação digital em nuvem NeoID | Por demanda | 1784 | R\$ 2.496,41 | R\$ 149.784,78 |
| Valor Total Mensal | | | | R\$ 2.496,41 |
| Valor Total 60 Meses | | | | R\$ 149.784,78 |

12. Descrição da solução de TIC a ser contratada

12.1. Conforme demonstrado neste Estudo Técnico, a solução consistente na contratação do serviço de certificação digital em nuvem NeoID, fornecido exclusivamente pelo SERPRO, revela-se a alternativa mais adequada e economicamente vantajosa para a DPU. A adoção do NeoID para um período contratual de 60 (sessenta) meses atende às necessidades institucionais, reduz custos operacionais, elimina a dependência de mídias físicas e garante maior eficiência, segurança e disponibilidade aos processos críticos da instituição.

12.2. Tabela de Composição da Solução

| Item | Descrição do Serviço | Métrica | Estimativa Mensal |
|------|--|---------|-------------------|
| 1 | Contratação de certificação digital em nuvem NeoID | USN | Por demanda |

13. Estimativa de custo total da contratação

Valor (R\$): 149.784,78

13.1 A estimativa do custo total da contratação foi elaborada com base nas definições da Instrução Normativa SEGES nº 65, de 7 de julho de 2021, e nas disposições aplicáveis às soluções de Tecnologia da Informação e Comunicação previstas na Instrução Normativa SGD nº 94, de 23 de dezembro de 2022.

13.2. Nesse sentido, os valores estimados abaixo estão de acordo com a Proposta Comercial encaminhada pelo SERPRO para o fornecimento do serviço de certificação digital em nuvem NeoID:

| Itens de Faturamento | Unidade de Medida | * Quantidade | Preço Unitário | Valor Total |
|---|---------------------|--------------|----------------|-----------------------|
| Certificado Digital - Com Imunidade - Varejo - PF - A3 (3 anos) com Token | Certificado Emitido | 60 | R\$ 241,16 | R\$ 14.469,60 |
| Certificado Digital - Com Imunidade - Varejo - PJ - A3 (3 anos) com Token | Certificado Emitido | 15 | R\$ 331,59 | R\$ 4.973,85 |
| Certificado Digital - Com Imunidade - Varejo - SerproID - PF - 3 anos | Certificado Emitido | 60 | R\$ 169,47 | R\$ 10.168,20 |
| Certificado Digital - Com Imunidade - Varejo - SerproID - PJ - 3 anos | Certificado Emitido | 15 | R\$ 235,41 | R\$ 3.531,15 |
| Certificação Digital - Emissão via Módulo Eletrônico de AR - PF A3 - 3 anos com Token | Certificado Emitido | 300 | R\$ 94,516 | R\$ 28.354,80 |
| Certificação Digital - Emissão via Módulo Eletrônico de AR - PF A3 - 3 anos | Certificado Emitido | 300 | R\$ 34,86 | R\$ 10.458,00 |
| SerproID - Emissão via Módulo Eletrônico de AR - PF e PJ - 3 anos | Certificado Emitido | 1034 | R\$ 75,27 | R\$ 77.829,18 |
| Total | | | | R\$ 149.784,78 |

14. Justificativa técnica da escolha da solução

14.1. A utilização de certificados digitais no âmbito da Administração Pública é imprescindível para garantir autenticidade, integridade e não repúdio em documentos e transações eletrônicas, conforme previsto na Medida Provisória nº 2.2002/2001, que instituiu a ICPBrasil. Diversos sistemas estruturantes do governo federal, como SIAPE, SIAFI, Compras.gov.br, SIGEPE, entre outros, exigem certificados digitais do tipo A3 para acesso seguro e assinatura de atos administrativos. Estudos técnicos de órgãos públicos corroboram essa necessidade, especialmente diante do crescente volume de documentos digitais que devem possuir validade jurídica.

14.2. Nesse contexto, a solução NeoID, ofertada pelo SERPRO, apresenta-se como alternativa tecnicamente superior ao modelo tradicional em token. Trata-se de certificado digital A3 em nuvem, cuja chave privada é gerada e protegida em módulo criptográfico seguro (HSM) na infraestrutura do próprio SERPRO. Essa arquitetura elimina o uso de dispositivos físicos, oferecendo maior disponibilidade, mobilidade e segurança. A solução permite o uso do certificado em computadores, smartphones e tablets, garantindo flexibilidade operacional e reduzindo substancialmente os problemas de perdas, danos ou incompatibilidades de tokens físicos, conforme amplamente demonstrado em estudos técnicos oficiais.

14.3. Além de atender integralmente aos requisitos normativos da ICPBrasil, a solução NeoID segue as práticas de segurança previstas em Declarações de Práticas de Certificação (DPC) e nas políticas de certificação vigentes, incluindo proteção em ambiente seguro, controles rigorosos de acesso e padrões compatíveis com as exigências das autoridades certificadoras. Isso assegura conformidade técnica e jurídica para atos administrativos digitais, alinhando-se às exigências dos órgãos públicos que utilizam certificados digitais como requisito indispensável para validação de procedimentos administrativos e processuais.

14.4. A contratação do NeoID também se justifica pela eficiência econômica e pela redução de riscos operacionais. A eliminação do token físico reduz custos de aquisição, reposição e suporte técnico, diminuindo a carga administrativa associada à manutenção desses dispositivos. A mobilidade proporcionada pela infraestrutura em HSM do SERPRO aumenta a produtividade dos servidores, especialmente em modelos de trabalho remoto ou híbrido. Estudos técnicos de referência apontam que certificados digitais em nuvem modernizam fluxos de trabalho, reduzem a burocracia, agilizam procedimentos e reforçam a segurança da informação institucional.

14.5. Assim, a contratação da certificação digital NeoID do SERPRO mostra-se tecnicamente fundamentada, atendendo às necessidades de segurança, mobilidade, conformidade normativa e eficiência operacional essenciais ao adequado funcionamento

das atividades institucionais que dependem de certificação digital. A solução contribui diretamente para a continuidade, confiabilidade e modernização dos processos digitais do órgão, oferecendo alternativa robusta, segura e alinhada às melhores práticas da Administração Pública.

15. Justificativa econômica da escolha da solução

15.1 A contratação da certificação digital NeoID do SERPRO apresenta-se economicamente vantajosa, pois reduz custos diretos e indiretos associados ao modelo tradicional de certificados A3 armazenados em tokens físicos. Estudos técnicos da Administração Pública demonstram que certificados em nuvem eliminam despesas recorrentes relacionadas à aquisição, manutenção, substituição e logística de entrega desses dispositivos, os quais estão sujeitos a desgaste, extravio, danos e incompatibilidades tecnológicas, demandando reposições frequentes que oneram o orçamento público. Ademais, a utilização de certificados digitais visa simplificar processos, reduzir burocracia e diminuir custos operacionais, alinhando-se aos princípios de economicidade e racionalização de gastos que orientam a gestão pública.

15.2. O modelo NeoID, por ser totalmente baseado em nuvem e apoiado por módulo criptográfico seguro (HSM), garante continuidade do serviço sem necessidade de infraestrutura física adicional e confere maior previsibilidade orçamentária. Desde a interrupção do custeio centralizado pelo governo federal, em 2017, cada órgão passou a ser responsável pelo próprio planejamento financeiro relacionado à certificação digital, o que reforça a relevância de soluções que reduzam investimentos em hardware e minimizem a necessidade de suporte técnico intensivo. A migração para certificados em nuvem reduz a demanda por atendimentos de TI, uma vez que elimina problemas de instalação, atualização de drivers e incompatibilidade de sistemas — pontos frequentemente apontados como causas de chamados e retrabalhos.

15.3. Outro aspecto econômico relevante é a mobilidade proporcionada pelo certificado armazenado em HSM, que permite assinaturas digitais em diferentes dispositivos e ambientes de trabalho, diminuindo atrasos em fluxos administrativos e aumentando a produtividade dos servidores. Essa agilidade operacional gera economia indireta significativa, pois reduz o tempo de tramitação de processos e previne interrupções de atividades críticas decorrentes da indisponibilidade de tokens físicos. Estudos de referência demonstram que a certificação digital contribui para a redução de custos administrativos ao possibilitar processos mais céleres, digitais e seguros, eliminando etapas presenciais e diminuindo a necessidade de recursos materiais.

15.4. Assim, sob a perspectiva econômica, a contratação da certificação digital NeoID do SERPRO é plenamente justificável, pois otimiza os gastos públicos ao reduzir despesas com dispositivos físicos, minimizar custos de suporte e manutenção, aumentar a eficiência dos fluxos de trabalho e elevar a produtividade institucional. Trata-se de solução financeiramente sustentável, alinhada às diretrizes de economicidade e eficiência que orientam as contratações de tecnologia da informação no setor público.

15.5. Do Parcelamento da Contratação Decorrente de Aspectos Econômicos

15.5.1. O objeto da contratação não comporta parcelamento, em razão de sua natureza tecnológica integrada e indivisível. A solução de certificação digital em nuvem demanda interoperabilidade entre componentes, gestão centralizada de identidades, uniformidade de padrões de segurança e governança unificada do serviço.

15.5.2. O eventual parcelamento comprometeria a eficiência operacional, aumentaria os riscos de inconsistências técnicas, dificultaria a gestão do contrato e poderia impactar negativamente a segurança da informação e a continuidade do serviço.

15.5.3. Dessa forma, a contratação integrada mostrase tecnicamente necessária e economicamente mais eficiente, nos termos do art. 18, §1º, inciso VIII, da Lei nº 14.133/2021.

16. Benefícios a serem alcançados com a contratação

16.1. A contratação do serviço de certificação digital em nuvem NeoID, fornecido exclusivamente pelo SERPRO, proporcionará uma série de benefícios estratégicos, operacionais e econômicos à Defensoria Pública da União (DPU), garantindo maior eficiência, segurança e continuidade dos serviços institucionais.

16.2. Dentre os principais benefícios, destacam-se:

16.2.1. Aumento da segurança da informação

16.2.1.1. Armazenamento de chaves privadas em HSM (Hardware Security Module) do SERPRO, impedindo migração, cópia ou extração do certificado;

16.2.1.2. Redução de riscos de extravio, dano físico ou vulnerabilidades associadas a tokens USB.

16.2.1.3. Conformidade integral com os requisitos da ICPBrasil e padrões de segurança aplicáveis ao setor público.

16.2.2. Continuidade e disponibilidade do serviço

16.2.2.1. Eliminação da dependência de mídias físicas, que podem quebrar, ser perdidas ou se tornar incompatíveis com novos sistemas.

16.2.2.2. Infraestrutura em nuvem com alta disponibilidade e redundância, garantindo acesso ao certificado independentemente do dispositivo.

16.2.3. Ganhos de eficiência operacional

16.2.3.1. Uso do certificado em múltiplos dispositivos (computador, celular, tablet), sem necessidade de drivers ou instalação de softwares adicionais.

16.2.3.2. Redução significativa de chamados de suporte relacionados a token, drivers e incompatibilidades.

16.2.3.3. Flexibilidade para assinaturas remotas, agilizando trâmites administrativos e processuais.

16.2.4. Redução de custos diretos e indiretos

16.2.4.1. Eliminação de despesas com compra, reposição e logística de tokens físicos.

16.2.4.2. Menor demanda por suporte técnico e menor necessidade de gestão de estoque de mídias.

16.2.4.3. Economia indireta pela aceleração de fluxos de trabalho e redução de retrabalhos.

16.2.5. Apoio ao trabalho remoto e híbrido

16.2.5.1. Mobilidade plena do certificado digital, permitindo autenticação e assinatura em qualquer local.

16.2.5.2. Maior produtividade dos servidores, especialmente nas atividades que dependem de assinatura digital contínua.

16.2.6. Conformidade regulatória e aderência às práticas de modernização

16.2.6.1. Aderência às diretrizes de transformação digital do Governo Federal.

16.2.6.2. Suporte nativo a sistemas estruturantes como SEI, PJe, eProc, Compras.gov.br, SIAFI, SIGEPE e demais plataformas integradas ao ecossistema gov.br.

16.2.6.3. Utilização de solução oficial do SERPRO, órgão federal especializado em serviços críticos de TI e infraestrutura segura.

16.2.7. Modernização dos processos internos

16.2.7.1. Redução da burocracia e eliminação de etapas físicas associadas ao uso de tokens.

16.2.7.2. Maior agilidade no trâmite de documentos, autorizações e processos eletrônicos.

16.2.7.3. Padronização do acesso digital, fortalecendo a governança de identidades na instituição.

16.2.8. Suporte à transformação digital da DPU

16.2.8.1. Contribuição direta para a digitalização dos fluxos administrativos.

16.2.8.2. Melhor experiência para servidores, membros e unidades administrativas.

16.2.8.3. Alinhamento às estratégias de eficiência, inovação e sustentabilidade tecnológica.

17. Providências a serem Adotadas

7.1. Para a presente contratação, serão adotadas as seguintes providências:

17.1.1. Levantamento de Requisitos: Identificação das necessidades e especificações técnicas.

17.1.2. Elaboração do Termo de Referência: Documento que detalha os requisitos, escopo e condições da contratação.

17.1.3. Elaboração de Mapa de Risco para o cenário escolhido neste estudo.

17.1.4. Implementação e Gestão do Contrato: Acompanhamento da execução dos serviços e gestão do contrato conforme as cláusulas estabelecidas.

17.2. Vinculação entre riscos e decisões do planejamento:

17.2.1. Os riscos identificados na Matriz de Riscos da contratação influenciaram diretamente as decisões adotadas no planejamento, especialmente no que se refere à escolha da solução tecnológica, à definição dos requisitos de segurança da informação, à exigência de alta disponibilidade do serviço e às medidas de continuidade operacional.

17.2.2. A seleção da solução NeoID considerou, de forma prioritária, a mitigação de riscos relacionados à indisponibilidade do serviço, à proteção de dados pessoais, à conformidade regulatória e à dependência tecnológica, refletindo na modelagem contratual e nos requisitos técnicos definidos.

17.2.3. Dessa forma, resta evidenciado que a gestão de riscos constituiu elemento orientador do planejamento da contratação, em conformidade com o art. 18 da Lei nº 14.133/2021, assegurando maior consistência técnica e aderência aos princípios do planejamento, da motivação e da eficiência administrativa.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1. Esta Equipe de Planejamento da Contratação, após a realização dos estudos técnicos, levantamento de mercado, análise comparativa das soluções disponíveis e avaliação dos aspectos técnicos, operacionais e econômicos, declara viável a presente contratação, considerando atendidos os requisitos de necessidade, adequação e vantajosidade para a Administração Pública.

18.2. Verificou-se que a solução de certificação digital em nuvem NeoID, fornecida pelo Serviço Federal de Processamento de Dados – SERPRO, é a única capaz de atender integralmente aos requisitos técnicos, de integração governamental, segurança da informação e interoperabilidade necessários ao pleno funcionamento dos sistemas utilizados pelo órgão.

18.3. A análise demonstrou que as demais soluções existentes no mercado não atendem simultaneamente às exigências técnicas e operacionais identificadas, seja por ausência de integração nativa com plataformas governamentais, seja por limitações de gestão centralizada de identidades ou inadequação aos padrões tecnológicos adotados pela Administração Pública Federal.

18.4. Sob o aspecto econômico, a solução em nuvem apresenta menor custo total de propriedade (TCO) ao longo do ciclo de vida da contratação, reduzindo despesas com hardware, suporte técnico, logística e manutenção, além de ampliar a disponibilidade e a produtividade institucional.

18.5. Diante do exposto, conclui-se pela viabilidade técnica, operacional e econômica da contratação, recomendando-se sua realização por dispensa de licitação, com fundamento no art. 75, inciso IX, da Lei nº 14.133/2021, em razão de se tratar de contratação de serviço prestado por empresa pública federal integrante da Administração Pública indireta, cuja solução atende diretamente às necessidades institucionais identificadas.

18.6. A contratação mostra-se alinhada aos princípios da eficiência, economicidade, continuidade do serviço público e transformação digital da Administração, bem como às diretrizes estabelecidas pela IN nº 94/2022/SGD, estando devidamente justificada nos presentes estudos técnicos.

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](#).

ROMULO AUGUSTO BRITTO KLEIN

Secretário de Tecnologia da Informação Substituto



Assinou eletronicamente em 09/04/2026 às 15:56:12.

JOELMA MARIA DE SOUSA BEZERRA FEITOSA

Secretária de Gestão de Pessoas



Assinou eletronicamente em 09/04/2026 às 15:49:00.