

INST FED. EDUC. CIENC. TEC. RJ/CAMP. REALENGO

Estudo Técnico Preliminar 5/2026

1. Informações Básicas

Número do processo: 23273.000115/2026-37

2. Descrição da necessidade

A presente demanda tem por objeto a contratação de empresa especializada para o fornecimento de certificados digitais do tipo A3 (e-cpf e e-cnpj), armazenados em nuvem (sem uso de token físico), destinados a atender às necessidades do órgão.

A contratação se faz necessária em razão da crescente digitalização dos processos administrativos e da obrigatoriedade de utilização de assinaturas digitais em sistemas oficiais do Governo Federal, como o gov.br, Comprasnet, SEI e demais plataformas institucionais.

A adoção de certificados digitais em nuvem visa proporcionar maior flexibilidade, mobilidade e segurança no acesso aos sistemas, permitindo que os usuários autorizados realizem assinaturas digitais e autenticações de forma remota, sem a dependência de dispositivos físicos, reduzindo riscos de perda, dano ou incompatibilidade de hardware.

Destaca-se, ainda, que a solução em nuvem possibilita melhor gestão dos certificados, com controle centralizado, facilidade de emissão, renovação e revogação, além de maior aderência às boas práticas de segurança da informação.

A ausência da contratação poderá comprometer a continuidade das atividades administrativas que dependem de certificação digital, ocasionando atrasos na tramitação de processos, prejuízos operacionais e eventual descumprimento de obrigações legais e institucionais.

Dessa forma, a contratação pretendida visa assegurar a continuidade, eficiência e segurança das atividades digitais do órgão, em conformidade com as diretrizes de transformação digital da Administração Pública.

3. Área requisitante

Área Requisitante	Responsável
DATE	Francisco Jorge Campos dos Anjos

4. Necessidades de Negócio

A presente contratação está diretamente alinhada à necessidade de garantir a continuidade e a eficiência das atividades administrativas do órgão, especialmente no que se refere à tramitação eletrônica de processos, assinatura de documentos digitais e acesso a sistemas estruturantes da Administração Pública Federal.

A utilização de certificados digitais em nuvem é essencial para viabilizar a atuação dos servidores em ambientes digitais, permitindo a realização de atos administrativos com validade jurídica, de forma segura, ágil e em conformidade com as exigências legais.

A solução contribui para o cumprimento das diretrizes de transformação digital, desburocratização e modernização da gestão pública, promovendo maior celeridade nos fluxos de trabalho, redução do uso de papel e aumento da produtividade institucional.

Além disso, a adoção de certificados digitais sem token físico favorece a mobilidade dos usuários, possibilitando o acesso remoto aos sistemas corporativos, o que se mostra especialmente relevante em cenários de trabalho híbrido ou remoto.

Ressalta-se que a indisponibilidade dessa solução pode impactar diretamente a execução das atividades finalísticas e administrativas do órgão, ocasionando atrasos, retrabalho e prejuízos à prestação de serviços públicos.

Dessa forma, a contratação atende a uma necessidade estratégica do negócio, ao assegurar meios adequados para a execução segura, eficiente e contínua das atividades institucionais.

5. Necessidades Tecnológicas

A contratação demanda solução tecnológica que viabilize a emissão e utilização de certificados digitais do tipo A3 em ambiente de nuvem, dispensando o uso de mídias físicas, como tokens ou cartões, e permitindo autenticação e assinatura digital com alto nível de segurança.

A solução deve estar aderente à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), garantindo validade jurídica, integridade, autenticidade e não repúdio das transações realizadas por meio dos certificados digitais.

Além disso, é necessária a utilização de mecanismos de segurança robustos, tais como autenticação multifator, criptografia e controle de acesso, assegurando a proteção das chaves privadas armazenadas em ambiente seguro e certificado.

A plataforma deve possibilitar gestão centralizada dos certificados, incluindo emissão, renovação, revogação e auditoria, bem como compatibilidade com os principais sistemas utilizados pela Administração Pública, a exemplo de sistemas de processo eletrônico, compras governamentais e demais aplicações que exijam autenticação digital.

Adicionalmente, a solução deve garantir alta disponibilidade, escalabilidade e acesso remoto, permitindo o uso dos certificados em diferentes dispositivos, sem prejuízo da segurança e da conformidade com as normas vigentes.

Dessa forma, a contratação envolve requisitos tecnológicos específicos, voltados à segurança da informação, interoperabilidade e continuidade dos serviços digitais do órgão.

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

Para a adequada seleção da solução de Tecnologia da Informação e Comunicação, deverão ser observados os seguintes requisitos, considerados necessários e suficientes ao atendimento da demanda:

a) Requisitos técnicos:

- Fornecimento de certificados digitais do tipo A3, com armazenamento em nuvem, sem utilização de mídia física (token ou cartão);
- Compatibilidade com os principais sistemas utilizados pela Administração Pública, incluindo o Comprasnet e demais sistemas que exijam autenticação via certificado digital;
- Conformidade com os padrões da ICP-Brasil;
- Disponibilidade de acesso seguro por múltiplos dispositivos autorizados;
- Utilização de mecanismos de segurança, como criptografia e autenticação multifator;
- Garantia de validade e integridade dos certificados durante todo o período contratado.

b) Requisitos operacionais:

- Emissão e disponibilização dos certificados de forma ágil, preferencialmente com validação remota;
- Disponibilidade de suporte técnico ao usuário durante todo o período de vigência;
- Facilidade de uso da plataforma de gestão dos certificados;
- Possibilidade de revogação e reemissão dos certificados, quando necessário;
- Garantia de continuidade do serviço, com níveis mínimos de disponibilidade.

c) Requisitos legais e normativos:

- Atendimento à Medida Provisória nº 2.200-2/2001, que institui a Infraestrutura de Chaves Públicas Brasileira;
- Observância às diretrizes da ITI;
- Conformidade com a Lei nº 14.133/2021, no que couber;
- Garantia de validade jurídica das assinaturas realizadas com o certificado.

d) Requisitos de segurança da informação:

- Proteção contra acessos não autorizados;
- Registro e rastreabilidade das operações realizadas com o certificado;
- Armazenamento seguro das chaves criptográficas;
- Conformidade com boas práticas de segurança da informação.

e) Requisitos de suporte e manutenção:

- Disponibilização de canais de atendimento ao usuário;
- Tempo de resposta adequado para resolução de incidentes;
- Atualizações e melhorias contínuas da solução sem ônus adicional, quando aplicável.

7. Estimativa da demanda - quantidade de bens e serviços

A estimativa da demanda foi realizada com base no quantitativo de servidores que necessitam utilizar certificados digitais para o desempenho de suas atribuições institucionais, especialmente para acesso a sistemas estruturantes do Governo Federal, como o Comprasnet, bem como para assinatura eletrônica de documentos com validade jurídica.

Considerando a atual estrutura administrativa do órgão e a necessidade de garantir a continuidade das atividades operacionais, estima-se a seguinte demanda:

- **Certificados digitais do tipo e- CPF A3 armazenado em nuvem:** 207 (duzentos e sete) unidades;
- **Certificados digitais do tipo e- CNPJ A3 armazenado em nuvem:** 12 (doze) unidades;
- **Validade dos certificados:** 36 meses;
- **Serviços associados:**
 - Emissão inicial dos certificados;
 - Validação de identidade (presencial ou remota);
 - Suporte técnico durante a vigência;
 - Revogação e eventual reemissão, quando necessário.

A definição do quantitativo considerou:

- Servidores que atuam diretamente com processos de compras, contratos e atividades administrativas;
- A necessidade de substituição de certificados vencidos ou próximos do vencimento;
- A ampliação do uso de certificação digital no âmbito do órgão.

Ressalta-se que os quantitativos poderão ser ajustados na fase de planejamento da contratação, caso haja alteração na estrutura organizacional ou na demanda institucional.

8. Levantamento de soluções

Foram analisadas as possíveis soluções disponíveis no mercado para atendimento da necessidade de certificação digital do tipo A3, considerando aspectos técnicos, operacionais, de segurança e de custo-benefício.

As principais alternativas identificadas são:

a) Certificado digital A3 em mídia física (token ou cartão):

Solução tradicional, na qual o certificado é armazenado em dispositivo criptográfico (token ou smartcard), exigindo uso físico e instalação de drivers específicos em cada equipamento.

Vantagens:

- Alto nível de segurança (armazenamento local da chave privada);
- Ampla aceitação e compatibilidade.

Desvantagens:

- Dependência de dispositivo físico (risco de perda, dano ou extravio);
- Necessidade de instalação e configuração em cada máquina;
- Dificuldade de uso remoto;
- Custos adicionais com aquisição de tokens.

b) Certificado digital A1 (arquivo):

Certificado armazenado diretamente no computador do usuário, com validade geralmente inferior (1 ano).

Vantagens:

- Facilidade de instalação e uso;
- Dispensa dispositivos físicos.

Desvantagens:

- Menor nível de segurança em comparação ao A3;
- Armazenamento vulnerável a cópias indevidas;
- Não recomendado para perfis com maior exigência de segurança institucional.

c) Certificado digital A3 em nuvem (sem token):

Solução moderna em que o certificado é armazenado em ambiente seguro na nuvem, com acesso controlado por autenticação forte.

Vantagens:

- Dispensa uso de mídia física;
- Possibilita acesso remoto e em múltiplos dispositivos;
- Maior praticidade e mobilidade para os usuários;
- Redução de custos operacionais com hardware;
- Elevado nível de segurança, com uso de criptografia e autenticação multifator;
- Gestão centralizada e facilitada.

Desvantagens:

- Dependência de conexão com a internet;
- Necessidade de adaptação inicial dos usuários.

d) Soluções disponibilizadas por Autoridades Certificadoras credenciadas:

Diversas entidades credenciadas junto à ICP-Brasil oferecem certificados digitais em nuvem, como:

- Serpro;
- Valid Certificadora;
- Certisign;
- Soluti.

Conclusão do levantamento:

Após análise das alternativas, verifica-se que a solução de **certificado digital do tipo A3 em nuvem** apresenta-se como a mais adequada às necessidades do órgão, por aliar segurança, praticidade, mobilidade e redução de custos operacionais, atendendo plenamente aos requisitos técnicos e institucionais.

9. Análise comparativa de soluções

Com base no levantamento de soluções disponíveis no mercado, foi realizada análise comparativa entre as alternativas identificadas, considerando critérios de segurança, custo, facilidade de uso, mobilidade, manutenção e aderência às necessidades institucionais.

1. Certificado A3 em mídia física (token/cartão)

- **Segurança:** Alta
- **Custo:** Médio a alto (aquisição de dispositivo + manutenção)
- **Mobilidade:** Baixa (dependência do dispositivo físico)
- **Facilidade de uso:** Média (exige instalação de drivers e configurações)
- **Manutenção:** Necessidade de suporte para problemas físicos e compatibilidade
- **Aderência à necessidade:** Parcial

2. Certificado A1 (arquivo digital)

- **Segurança:** Média
- **Custo:** Baixo
- **Mobilidade:** Alta
- **Facilidade de uso:** Alta
- **Manutenção:** Baixa complexidade
- **Aderência à necessidade:** Parcial (não recomendado para maior nível de segurança institucional)

3. Certificado A3 em nuvem (sem token)

- **Segurança:** Alta (com autenticação multifator e armazenamento seguro)
- **Custo:** Médio (sem necessidade de hardware adicional)
- **Mobilidade:** Alta (acesso remoto e multiplataforma)
- **Facilidade de uso:** Alta
- **Manutenção:** Baixa (gestão centralizada pelo fornecedor)
- **Aderência à necessidade:** Total

Adicionalmente, as soluções em nuvem disponibilizadas por Autoridades Certificadoras credenciadas junto à ICP-Brasil, como Serpro, Certisign e Valid Certificadora, demonstram elevado grau de maturidade, confiabilidade e conformidade normativa.

Conclusão da análise comparativa:

Diante dos critérios avaliados, verifica-se que o **certificado digital do tipo A3 em nuvem** apresenta a melhor relação entre segurança, eficiência operacional e custo-benefício, sendo a solução que mais adequadamente atende às necessidades do órgão.

A escolha dessa solução justifica-se pela eliminação da dependência de dispositivos físicos, maior flexibilidade de uso, facilidade de gestão e aderência às práticas modernas de transformação digital no âmbito da Administração Pública.

10. Registro de soluções consideradas inviáveis

Durante o processo de levantamento e análise das alternativas disponíveis no mercado, algumas soluções foram consideradas inviáveis para atendimento da necessidade institucional, conforme descrito a seguir:

a) Certificado digital do tipo A1 (arquivo digital):

Embora apresente facilidade de uso e menor custo inicial, esta solução foi considerada inviável em razão do nível de segurança inferior, uma vez que a chave privada fica armazenada no próprio dispositivo do usuário, tornando-se mais suscetível a cópias indevidas, acessos não autorizados e comprometimento das credenciais.

Adicionalmente, tal solução não é a mais adequada para atividades institucionais que demandam maior grau de segurança e validade jurídica reforçada.

b) Certificado digital A3 em mídia física (token ou cartão):

Apesar de oferecer elevado nível de segurança, esta alternativa foi considerada inviável devido às limitações operacionais, tais como:

- Dependência de dispositivo físico para utilização;
- Risco de extravio, dano ou bloqueio do token;
- Necessidade de instalação e configuração em cada equipamento;
- Dificuldade de utilização em trabalho remoto ou em múltiplos dispositivos;
- Custos adicionais relacionados à aquisição e eventual substituição dos dispositivos.

Tais fatores impactam negativamente a eficiência operacional e a continuidade das atividades administrativas.

c) Soluções não compatíveis com a ICP-Brasil:

Foram desconsideradas quaisquer soluções que não estejam em conformidade com os padrões estabelecidos pela Infraestrutura de Chaves Públicas Brasileira, por não atenderem aos requisitos legais de validade jurídica das assinaturas eletrônicas no âmbito da Administração Pública, conforme disposto na Medida Provisória nº 2.200-2/2001.

Conclusão:

As soluções acima foram consideradas inviáveis por não atenderem, de forma integral, aos requisitos de segurança, mobilidade, eficiência operacional e conformidade normativa exigidos pelo órgão, restando como alternativa mais adequada a adoção de certificados digitais do tipo A3 em nuvem.

11. Análise comparativa de custos (TCO)

A análise de custo total de propriedade (Total Cost of Ownership – TCO) foi realizada considerando não apenas o custo de aquisição dos certificados digitais, mas também os custos indiretos relacionados à operação, manutenção, suporte e eventuais perdas ou substituições ao longo do período de utilização.

Foram comparadas as principais alternativas identificadas:

1. Certificado A3 em mídia física (token/cartão):

Custos diretos:

- Aquisição do certificado digital;
- Aquisição do dispositivo criptográfico (token ou smartcard).

Custos indiretos:

- Substituição de dispositivos em caso de perda, dano ou defeito;
- Suporte técnico para instalação e configuração;

- Tempo de indisponibilidade em caso de falhas;
- Custos operacionais relacionados à gestão de dispositivos físicos.

TCO estimado: Alto, considerando a necessidade de aquisição e manutenção de hardware, além dos custos operacionais associados.

2. Certificado A1 (arquivo digital):

Custos diretos:

- Aquisição do certificado digital.

Custos indiretos:

- Riscos associados à segurança da informação;
- Possíveis custos decorrentes de incidentes de segurança (comprometimento de credenciais);
- Necessidade de renovação mais frequente (geralmente anual).

TCO estimado: Baixo a médio, porém com riscos elevados que podem gerar custos indiretos significativos.

3. Certificado A3 em nuvem (sem token):

Custos diretos:

- Contratação do certificado digital em nuvem.

Custos indiretos:

- Baixos custos de suporte, geralmente incluídos na contratação;
- Ausência de custos com aquisição e manutenção de dispositivos físicos;
- Redução de tempo de indisponibilidade;
- Menor necessidade de suporte técnico interno.

TCO estimado: Médio, com tendência a redução ao longo do tempo devido à eliminação de custos operacionais e maior eficiência.

Análise consolidada:

Embora o custo inicial do certificado A3 em nuvem possa ser equivalente ou ligeiramente superior ao do certificado A1, a análise do custo total de propriedade demonstra maior economicidade ao longo do tempo, especialmente quando comparado à solução com mídia física.

A solução em nuvem elimina custos relacionados à aquisição, reposição e gestão de dispositivos físicos, além de reduzir significativamente os riscos operacionais e de segurança.

Adicionalmente, soluções fornecidas por Autoridades Certificadoras credenciadas junto à ICP-Brasil, como Serpro e Certisign, já incluem suporte técnico e infraestrutura necessária, contribuindo para a previsibilidade dos custos.

Conclusão:

Diante da análise de TCO, a solução de **certificado digital do tipo A3 em nuvem** apresenta a melhor relação custo-benefício, sendo a alternativa mais vantajosa sob a ótica econômica e operacional para a Administração Pública.

12. Descrição da solução de TIC a ser contratada

A solução de Tecnologia da Informação e Comunicação a ser contratada consiste no fornecimento de **certificados digitais do tipo A3, com armazenamento em nuvem**, em conformidade com os padrões da ICP-Brasil, destinados à autenticação e assinatura eletrônica de documentos no âmbito institucional.

A contratação compreenderá:

- **Fornecimento de 10 (dez) certificados digitais A3 em nuvem**, vinculados a pessoas físicas (e-CPF), destinados a servidores autorizados;
- **Validade dos certificados:** a definir (preferencialmente 12 ou 36 meses, conforme vantajosidade);
- **Serviços de emissão e validação de identidade**, podendo ser realizados de forma presencial ou remota;
- **Disponibilização de plataforma segura para utilização dos certificados**, com acesso controlado e autenticação multifator;
- **Suporte técnico durante toda a vigência contratual**;
- **Serviços de revogação e reemissão**, quando necessário.

A solução deverá permitir:

- Utilização dos certificados em múltiplos dispositivos autorizados;
- Acesso remoto seguro;
- Assinatura digital de documentos com validade jurídica, conforme a Medida Provisória nº 2.200-2/2001;
- Compatibilidade com sistemas governamentais, como o Comprasnet e demais sistemas institucionais.

Adicionalmente, a solução deverá garantir:

- Armazenamento seguro das chaves criptográficas;
- Registro e rastreabilidade das operações realizadas;
- Alta disponibilidade do serviço;
- Conformidade com normas de segurança da informação.

Fechamento:

A solução proposta atende integralmente às necessidades do órgão, proporcionando maior segurança, mobilidade, eficiência operacional e aderência às diretrizes de transformação digital da Administração Pública.

13. Estimativa de custo total da contratação

Valor (R\$): 2.113,80

A estimativa de custo total da contratação foi elaborada com base em pesquisa de mercado junto a fornecedores de certificados digitais credenciados na ICP-Brasil, considerando contratações similares realizadas por órgãos públicos e valores praticados por empresas como Serpro, Certisign e Valid Certificadora.

Com base nos levantamentos realizados, estima-se o valor médio unitário de:

- **Certificado digital, tipo e-cpf A3 armazenado em nuvem:** R\$ 162,60 (cento e sessenta e dois reais e sessenta centavos)

Considerando a demanda de **207(duzentos e sete) certificados**, tem-se:

- **Custo total estimado da contratação:** R\$ 33.658,20 (trinta e tres mil, seiscentos e cinquenta e oito reais e vinte centavos.)
- **Certificado digital, tipo e-cnpj A3 armazenado em nuvem:** R\$ 148,73 (cento e quarenta e oito reais e setenta e tres centavos)
- Considerando a demanda de **12(doze) certificados**, tem-se:
- **Custo total estimado da contratação:** R\$ 1784,76 (mil setecentos e oitenta e quatro e setenta e seis);

A estimativa contempla:

- Emissão dos certificados digitais;
- Validação de identidade dos titulares;
- Disponibilização da solução em nuvem;
- Suporte técnico durante a vigência;
- Eventuais serviços de revogação e reemissão.

Ressalta-se que os valores apresentados são estimativos e poderão variar conforme proposta mais vantajosa obtida no processo licitatório, observando-se os princípios da economicidade e da seleção da proposta mais vantajosa para a Administração Pública, conforme a Lei nº 14.133/2021.

14. Justificativa técnica da escolha da solução

A escolha da solução de **certificado digital do tipo A3 com armazenamento em nuvem** fundamenta-se em critérios técnicos, operacionais, de segurança da informação e de custo-benefício, conforme análise realizada ao longo deste Estudo Técnico Preliminar.

Do ponto de vista **técnico**, a solução atende integralmente aos requisitos de segurança exigidos, com utilização de criptografia robusta, armazenamento seguro das chaves privadas em ambiente controlado e mecanismos adicionais, como autenticação multifator, garantindo elevado nível de proteção contra acessos não autorizados.

Sob o aspecto **operacional**, a solução em nuvem elimina a necessidade de utilização de dispositivos físicos (tokens ou cartões), reduzindo riscos de perda, extravio ou dano, além de permitir o uso dos certificados em múltiplos dispositivos autorizados, com acesso remoto seguro. Tal característica proporciona maior flexibilidade e eficiência no desempenho das atividades institucionais.

No que se refere à **conformidade normativa**, a solução está plenamente aderente aos padrões estabelecidos pela ICP-Brasil, assegurando a validade jurídica das assinaturas eletrônicas, conforme previsto na Medida Provisória nº 2.200-2/2001.

Além disso, a solução apresenta elevada **compatibilidade com sistemas governamentais**, como o Comprasnet, garantindo plena integração com as ferramentas utilizadas pelo órgão.

Sob a ótica **econômica**, a análise do custo total de propriedade (TCO) demonstrou que a solução em nuvem reduz custos indiretos relacionados à aquisição e manutenção de dispositivos físicos, suporte técnico e indisponibilidade operacional, apresentando melhor relação custo-benefício ao longo do tempo.

Por fim, a solução está alinhada às diretrizes de **transformação digital da Administração Pública**, promovendo modernização, eficiência, mobilidade e segurança na execução das atividades administrativas.

Conclusão:

Diante dos aspectos analisados, conclui-se que a contratação de certificados digitais do tipo A3 em nuvem é tecnicamente adequada, suficiente e a mais vantajosa para atender às necessidades do órgão.

15. Justificativa econômica da escolha da solução

A escolha da solução de **certificado digital do tipo A3 em nuvem** mostra-se economicamente mais vantajosa para a Administração, conforme demonstrado na análise de custo total de propriedade (TCO) realizada neste Estudo Técnico Preliminar.

Embora o custo unitário da solução em nuvem possa ser equivalente ou ligeiramente superior a alternativas como o certificado do tipo A1, a análise global evidencia redução significativa de custos indiretos ao longo do período de utilização.

Diferentemente da solução baseada em mídia física (token ou cartão), a alternativa em nuvem elimina despesas relacionadas à aquisição, reposição e manutenção de dispositivos criptográficos, bem como reduz custos operacionais associados à instalação, configuração e suporte técnico.

Adicionalmente, a solução adotada proporciona:

- Redução de custos com suporte técnico interno;
- Minimização de riscos de indisponibilidade por falhas físicas ou extravio de dispositivos;
- Maior eficiência operacional dos usuários, com impacto positivo indireto na produtividade;
- Previsibilidade de custos, uma vez que os serviços geralmente são ofertados de forma integrada (emissão, suporte e gestão).

A solução também reduz potenciais custos decorrentes de incidentes de segurança, ao oferecer mecanismos mais robustos de proteção, em conformidade com os padrões da ICP-Brasil.

Considerando a estimativa de **R\$ 56.142,96 (cinquenta e seis mil cento e quarenta e dois reais e noventa e seis centavos)** para atendimento integral da demanda de 219 certificados, verifica-se que o investimento é compatível com os valores praticados no mercado e proporcional aos benefícios gerados.

Conclusão:

Dessa forma, conclui-se que a solução escolhida apresenta a melhor relação custo-benefício, sendo economicamente viável e vantajosa para a Administração Pública, em consonância com os princípios da economicidade e da eficiência previstos na Lei nº 14.133/2021.

16. Benefícios a serem alcançados com a contratação

A contratação da solução de **certificados digitais do tipo A3 em nuvem** proporcionará diversos benefícios à Administração Pública, tanto do ponto de vista operacional quanto estratégico, conforme descrito a seguir:

a) Aumento da segurança da informação:

A utilização de certificados digitais em nuvem, em conformidade com os padrões da ICP-Brasil, garante maior proteção das chaves criptográficas, com uso de mecanismos avançados como criptografia e autenticação multifator, reduzindo riscos de acessos indevidos e fraudes.

b) Maior eficiência operacional:

A eliminação da dependência de dispositivos físicos (tokens) permite maior agilidade no uso dos certificados, reduzindo o tempo necessário para execução de atividades como assinatura de documentos e acesso a sistemas institucionais.

c) Mobilidade e flexibilidade:

A solução possibilita o acesso remoto seguro e o uso em múltiplos dispositivos autorizados, facilitando o trabalho remoto e o desempenho das atividades fora do ambiente físico do órgão.

d) Redução de custos operacionais:

A dispensa de aquisição e manutenção de dispositivos físicos reduz custos indiretos, além de minimizar despesas com suporte técnico e substituição de equipamentos.

e) Continuidade dos serviços:

A solução em nuvem reduz riscos de indisponibilidade causados por perda, dano ou falha de dispositivos físicos, garantindo maior continuidade das atividades administrativas.

f) Conformidade legal e validade jurídica:

A solução assegura a validade jurídica das assinaturas eletrônicas, conforme a Medida Provisória nº 2.200-2/2001, sendo plenamente compatível com sistemas oficiais como o Comprasnet.

g) Alinhamento à transformação digital:

A adoção da solução contribui para a modernização dos processos administrativos, em consonância com as diretrizes de governo digital, promovendo maior eficiência, transparência e sustentabilidade.

Conclusão:

Os benefícios esperados demonstram que a contratação contribuirá significativamente para o aprimoramento das atividades institucionais, garantindo maior segurança, eficiência e economicidade na gestão pública.

17. Providências a serem Adotadas

Não há necessidade adicional de providências a serem adotadas para a contratação da solução.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

Com base nas análises realizadas neste Estudo Técnico Preliminar, conclui-se que a contratação de **certificados digitais do tipo A3 em nuvem é viável técnica e economicamente**, atendendo às necessidades do órgão.

A solução está em conformidade com as normas da ICP-Brasil e com a Lei nº 14.133/2021, além de apresentar adequada relação custo-benefício.

Dessa forma, recomenda-se o prosseguimento 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](#).

FRANCISCO JORGE CAMPOS DOS ANJOS

Membro da comissão de contratação



Assinou eletronicamente em 14/05/2026 às 05:09:40.

