MJ-CGS-COORDENACAO GERAL DE LOGISTICA/DF

Estudo Técnico Preliminar 47/2025

1. Informações Básicas

Número do processo: 08006.000386/2025-78

2. Descrição da necessidade

2.1. Contextualização Geral

2.1.1 O Ministério da Justiça e Segurança Pública (MJSP) necessita contratar serviços de certificação digital com o objetivo de garantir a continuidade, legalidade e segurança de suas operações no ambiente eletrônico. A certificação digital é elemento fundamental na gestão pública moderna, possibilitando a autenticação eletrônica segura de usuários, sistemas, equipamentos e entidades jurídicas. Essa tecnologia confere validade jurídica às assinaturas digitais, assegura comunicações protegidas entre sistemas e garante acesso restrito a plataformas críticas do governo. A ausência ou interrupção desses serviços impactaria diretamente a integridade de processos administrativos, a legalidade de atos digitais e a proteção de dados sensíveis, comprometendo a continuidade dos serviços públicos prestados à sociedade.

2.2. Necessidade e motivação da contratação

2.2.1. No âmbito do MJSP, os certificados digitais são amplamente utilizados por servidores, gestores, autoridades e sistemas automatizados. Constituem requisito técnico para o acesso a sistemas estruturantes do Governo Federal, como SEI, SCDP, SIASG, SICAF, SIAPE, SIGEP e SIAFI, entre outros. Também viabilizam a assinatura de documentos com validade legal, eliminando o uso de papel e promovendo eficiência, rastreabilidade e economia. Além disso, integram a política de segurança da informação da Pasta, garantindo os princípios de **integridade** (proteção contra alteração indevida de dados), **autenticidade** (confirmação da autoria), **confidencialidade** (proteção contra acessos não autorizados) e **não repúdio** (impossibilidade de negar a autoria), fundamentais para a confiança e governança nos processos institucionais.

2.2.2. Atualmente, esses serviços são prestados com base no Contrato Administrativo nº 13/2021, firmado com o Serviço Federal de Processamento de Dados (SERPRO), com vigência até março de 2026. Diante da impossibilidade de prorrogação contratual e considerando os previstos na Lei nº 14.133 /2021 para planejamento e tramitação de novas contratações, é imprescindível iniciar o processo para garantir a continuidade do fornecimento. A interrupção do serviço inviabilizaria sistemas essenciais, a tramitação eletrônica de documentos e atividades críticas internas e externas.

2.2.3. A nova contratação abrangerá diferentes tipos de certificados, incluindo **e-CPF** e **e-CNPJ** (para identificação de pessoas físicas e jurídicas).A solução contemplará também **certificados SSL/TLS para aplicações especiais**, destinados a **portais institucionais, APIs e serviços de integração**. Esses certificados **autenticam a identidade dos serviços web do MJSP e viabilizam a conexão criptografada (HTTPS)** entre servidores e usuários /sistemas consumidores, assegurando a **confidencialidade e integridade** dos dados em trânsito e elevando o nível de confiança das transações digitais do órgão.

2.2.4. Do ponto de vista normativo, a contratação seguirá a obrigatoriedade de adesão à **Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)**, prevista na Medida Provisória nº 2.200-2/2001, além das exigências da **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)**, da **Instrução Normativa SGD/ME nº 94/2022** e das diretrizes estratégicas institucionais. O aumento das demandas digitais, a expansão da base de usuários, a entrada de novos servidores e a modernização de processos justificam a estimativa de acréscimo de até 40% no quantitativo contratado em relação ao histórico recente.

2.2.5. Em síntese, trata-se de uma contratação **estratégica, essencial e inadiável** para assegurar a transformação digital e a prestação segura e eficiente de serviços à população, preservando a segurança jurídica, a conformidade normativa e a eficiência da gestão pública no MJSP.

2.3. Alinhamento com o Plano de Contratações Anual de 2025

2.3.1. O objeto da contratação está previsto no Plano de Contratações Anual de 2025 - MJSP, conforme tabela a seguir, bem como pode ser consultado através do link do PNCP (https://pncp.gov.br/app/pca/00394494000136/2025/52):

Classe	**Grupo**	Identificador	**Valor previsto da contratação.**

167	SERVIÇOS DE EMISSÃO DE CERTIFICADOS DIGITAIS	200005-18/2025	R$ 150.000,00

2.4. Alinhamento com Estratégias de Governo

2.4.1. De acordo com o Planejamento Estratégico Institucional 2024-2027 (PEI 2024-2027), o MJSP possui os seguintes objetivos estratégicos, entre outros:

2.4.1.1. Promover o acesso à justiça e proteger os direitos do cidadão, inclusive os digitais e os dados pessoais (OE. PEI.02);

2.4.1.2. Potencializar e aprimorar a estrutura e os serviços de Tecnologia da Informação e Comunicação (OE. PEI.09).

2.4.2. A Estratégia Federal de Governo Digital 2024-2027 (EFGD 2024-2027), formalizada pelo Decreto 12.198/2024 e Portaria SGD/MGI nº 6.618 /2024, está organizada em princípios, objetivos e iniciativas que nortearão a transformação do governo por meio do uso de tecnologias digitais e estabelece entre seus objetivos:

1. Prover serviços públicos digitais personalizados, simples, de forma proativa e centrados no cidadão (EFGD. 01);
2. Aperfeiçoar a governança de dados e a interoperabilidade (EFGD. 03);
3. Fomentar o uso inteligente de dados pelos órgãos do governo (EFGD. 06);
4. Desenvolver habilidades digitais dos servidores (EFGD. 08);
5. Elevar a maturidade e a resiliência dos órgãos e das entidades em termos de privacidade e segurança da informação (EFGD. 09);
6. Aprimorar processos de negócio da gestão pública (EFGD. 15).

2.4.3. O Plano Diretor de Tecnologia da Informação e Comunicação 2024-2027 – PDTIC 2024-2027 (SEI nº 31081525), aprovado pelo Comitê de Governança Digital e Segurança da Informação – CGDSIC do MJSP em sua 11ª reunião ordinária (SEI nº 31081526), traz o planejamento de TIC desenvolvido nos níveis estratégico e tático entre a área de TIC e as áreas finalísticas do órgão, alinhado aos objetivos estratégicos do PEI 2024-2027 do MJSP, de forma a orientar a aplicação dos recursos disponíveis de TIC com racionalidade, sustentabilidade, flexibilidade, agilidade e eficiência.

2.4.4. O PDTIC 2024-2027 possui abrangência aos órgãos de assistência direta e imediata ao Ministro de Estado da Justiça e Segurança Pública e aos órgãos específicos singulares, à exceção de Polícia Federal – PF, Polícia Rodoviária Federal – PRF, Conselho Administrativo de Defesa Econômica – CADE e Agência Nacional de Proteção de Dados – ANPD, que possuem PDTIC próprios.

2.4.5. Entre as diretrizes estabelecidas no PDTIC 2024-2027 está o fortalecimento e ampliação da estrutura e serviços de TI, por meio de investimento em recursos de TIC, visando o aumento da produtividade, a otimização dos recursos humanos utilizando inteligência artificial e aumento dos processos de segurança da informação, segurança e governança dos dados.

2.4.6. O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2024-2027, segue as diretrizes do DECRETO Nº 12.198, DE 24 DE SETEMBRO DE 2024.

Código Necessidade	Descrição	Ação Nº
N5513	Serviços de fornecimento de certificado digital A1 (máquina) e A3 (pessoal) para atendimento das necessidades de autenticação digital dos servidores e ativos do MJSP	A5513

2.5. Alinhamento a Plataforma gov.br - Inciso III, art. 6º da IN SGD 94/2022

2.5.1. A Contratação está alinhada com o DECRETO Nº 11.797, DE 27 DE NOVEMBRO DE 2023, que dispõe sobre o Serviço de Identificação do Cidadão e sobre a governança da identificação das pessoas naturais no âmbito da administração pública federal direta, autárquica e fundacional, institui a Câmara-Executiva Federal de Identificação do Cidadão - Cefic.

2.5.2. Os serviços que se pretende contratar levam em consideração as questões da segurança da informação, da ética, e os preceitos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD.

2.5.3. Por ser órgão também com atribuições de segurança pública, as especificações dos serviços, os requisitos de segurança e de privacidade da informação, e as necessidades de negócios, levam em consideração o possível compartilhamento de dados entre as instituições públicas.

2.5.4. Em observação ao art. 3º do Decreto nº 8.540/15: Trata-se de contratação de serviço essencial para o Órgão, com impacto positivo sobre a sociedade como um todo, a falta dos serviços pode impactar a segurança de infraestrutura, ambientes, sistemas e serviços prestados para as atividades do Ministério da Justiça e Segurança Pública no exercício de suas funções institucionais, bem como aqueles à sociedade.

2.5.5. A STI não dispõe de quadro próprio de pessoal especializado em TI em quantidade suficiente para a execução dos serviços especializados de segurança, por isso existe a necessidade da contratação proposta no objeto do Documento de Formalização da Demanda (SEI nº 32264827). Cabe informar que a execução indireta destes serviços está amparada na legislação específica, citando a autorização direta consubstanciada nos termos do Decreto nº 9.507, de 21 de setembro de 2018, conforme descrito abaixo:

"Art. 3º Não serão objeto de execução indireta na administração pública federal direta, autárquica e fundacional, os serviços:
I - que envolvam a tomada de decisão ou posicionamento institucional nas áreas de planejamento, coordenação, supervisão e controle;
II - que sejam considerados estratégicos para o órgão ou a entidade, cuja terceirização possa colocar em risco o controle de processos e de conhecimentos e tecnologias;
III - que estejam relacionados ao poder de polícia, de regulação, de outorga de serviços públicos e de aplicação de sanção; e
IV - que sejam inerentes às categorias funcionais abrangidas pelo plano de cargos do órgão ou da entidade, exceto disposição legal em contrário ou quando se tratar de cargo extinto, total ou parcialmente, no âmbito do quadro geral de pessoal.
§1º Os serviços auxiliares, instrumentais ou acessórios de que tratam os incisos do caput poderão ser executados de forma indireta, vedada a transferência de responsabilidade para a realização de atos administrativos ou a tomada de decisão para o contratado."

2.5.6. A pretendida contratação se enquadra como solução de TIC conforme disposto no inciso VII do art. 2º da Instrução Normativa nº 94/2022: conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos de TIC, de acordo com as premissas definidas no Anexo II desta Instrução Normativa.

2.5.6.1. O objeto da contratação não se enquadra nas vedações previstas nos artigos 3º, 4º e 5º da Instrução Normativa SGD/ME nº 94 /2022, pois:

a) trata-se de solução única de TIC;
b) não envolve terceirização de atividades estratégicas ou decisórias;
c) não há contratação por posto de trabalho ou homem-hora;
d) não há avaliação da solução pelo próprio fornecedor;
e) a remuneração está vinculada à entrega de certificados efetivamente emitidos.

2.5.6.2. Ademais, os serviços a serem contratados possuem natureza continuada, uma vez que são altamente relevantes para manter a segurança da infraestrutura e sistemas do MJSP, na manutenção da proteção cibernética dos serviços e dos dados corporativos do órgão.

2.5.6.3. Por fim, tendo em vista que a demanda em questão se trata de um serviço continuado e visando o cumprimento do Princípio da Continuidade do Serviço Público, entende-se necessária a contratação de empresa para prestação de serviços gerenciados de segurança da informação, a fim de que haja a continuidade dos serviços de proteção dos ativos de TIC, visando garantir a missão institucional do Ministério da Justiça e Segurança Pública.

3. Área requisitante

Área Requisitante	Responsável
CGISO/STI/SE	Leonardo Garcia Greco
CINF/CGISO/STI/SE	Artur Henrique Castro de Andrade

4. Necessidades de Negócio

4.1. A transformação digital em curso no Ministério da Justiça e Segurança Pública (MJSP) demanda mecanismos seguros de identificação, autenticação e assinatura digital, fundamentais para assegurar a confiabilidade das operações e a integridade das informações. A certificação digital é a principal tecnologia adotada para garantir autenticidade, rastreabilidade e validade jurídica em acessos, transações e documentos eletrônicos.

4.2. A ausência desse recurso inviabilizaria, por exemplo, a utilização segura de sistemas estruturantes da Administração Pública Federal, a assinatura digital de atos oficiais e o controle de acessos sensíveis a sistemas internos, expondo a instituição a riscos operacionais e jurídicos. Além disso, a certificação digital possibilita ganhos de eficiência administrativa, como a eliminação de documentos físicos, redução de retrabalho, automatização de processos e cumprimento de requisitos legais previstos na Lei nº 14.063/2020 (Assinaturas Eletrônicas) e na Lei nº 13.709/2018 (LGPD).

4.3. A exigência normativa recente da Secretaria do Tesouro Nacional — que impõe o uso de certificado digital, inclusive em nuvem, para autenticação no SIAFI a partir de abril de 2024 (comunicado STN, doc. SEI nº 28267217) — reforça a urgência da adequação tecnológica. Essa demanda envolve certificados tradicionais (e-CPF e e-CNPJ), certificados AE-S (Aplicações Específicas - Software) para autenticação de aplicações e máquinas, e certificados SSL/TLS para proteção de comunicações e transações em sistemas institucionais.

4.4. No caso do e-CNPJ, a necessidade não se limita à unidade matriz. Conforme comunicados da STN e documentos internos do MJSP (Siafi 2023 /3710482 – 27530532, 2024/3357021 – 27530540, 2024/3357158 – 27530542, 2024/3360791 – 27530547 e comunicado oficial da STN – 28267217), a Pasta possui atualmente 90 inscrições de CNPJ para unidades filiais e três CNPJs vinculados a Fundos Públicos (Senasp, Funad e FDD), demandando múltiplos certificados para representação institucional em sistemas federais, estaduais e municipais, como DETRANS e fiscos municipais.

4.5. A contratação visa garantir a continuidade dos serviços públicos, a integridade dos sistemas, a conformidade com a ICP-Brasil (MP nº 2.200-2 /2001) e com as diretrizes de governança digital, contribuindo para metas institucionais de modernização, segurança cibernética, sustentabilidade e racionalização de recursos. A previsão é de aumento de cerca de 40% na demanda em relação ao contrato atual, impulsionado pela ampliação da digitalização, ingresso de novos servidores e novas obrigatoriedades legais.

4.6. Dessa forma, a manutenção e expansão da infraestrutura de certificação digital é medida crítica, estratégica e inadiável, assegurando o funcionamento pleno das atividades do MJSP, a proteção da informação pública e o cumprimento das obrigações normativas vigentes. A demanda consta no Inventário de Necessidades do PDTIC 2024–2027, evidenciando seu alinhamento ao planejamento estratégico de TIC da instituição.

5. Necessidades Tecnológicas

5.1. Para atender à crescente demanda por segurança, autenticidade e integridade nas transações eletrônicas do Ministério da Justiça e Segurança Pública (MJSP), é necessário dispor de uma infraestrutura tecnológica robusta e compatível com as exigências normativas e operacionais vigentes.

5.2. A solução a ser contratada deve contemplar:

5.2.1. Conformidade com a ICP-Brasil

5.2.1.1. A solução deve estar em conformidade com os padrões da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, instituída pela Medida Provisória nº 2.200-2/2001, garantindo validade jurídica às assinaturas digitais e reconhecimento dos certificados em todo o território nacional.

5.2.2. Tipos de Certificados Necessários

5.2.2.1. Os certificados devem possuir validade compatível com o tipo contratado (ex.: 1 ano ou 3 anos) e estar disponíveis em mídias apropriadas (token criptográfico ou nuvem).

5.2.2.2. A contratação deverá abranger os seguintes tipos de certificados digitais:

- **e-CPF**: para identificação de servidores e assinatura de atos e documentos eletrônicos.
- **e-CNPJ**: para representação institucional da matriz e das 90 unidades filiais, bem como dos três fundos públicos (Senasp, Funad e FDD), em sistemas federais, estaduais e municipais.
- **Certificados SSL/TLS para aplicações especiais**: certificados para proteger portais, APIs e interfaces de integração do MJSP, **autenticando a identidade do serviço web e habilitando a conexão criptografada (HTTPS)**, preservando confidencialidade e integridade em trânsito.

5.2.3. Integração com Sistemas Estruturantes e Setoriais

5.2.3.1. A tecnologia deverá possibilitar a utilização dos certificados digitais nos principais sistemas utilizados pelo MJSP, incluindo:

- SIAFI (em conformidade com as novas exigências da STN para uso de certificado digital, inclusive em nuvem);
- SEI (Sistema Eletrônico de Informações);
- Sistemas corporativos de gestão de pessoas, finanças, patrimônio e logística;
- Portais de comunicação institucional e serviços online ao cidadão.

5.2.4. Suporte à Emissão e Gerenciamento em Ambiente Corporativo

5.2.4.1. A tecnologia deverá possibilitar recursos de gestão segura associados:

- Processo simplificado e seguro para emissão, renovação e revogação de certificados;
- Gestão centralizada, com rastreabilidade de uso e controles de auditoria;
- Suporte a múltiplas mídias de armazenamento (token USB, cartão, HSM e nuvem).

5.2.5. Segurança e Conformidade

5.2.5.1. A tecnologia deverá possibilitar recursos de segurança e conformidade, incluindo:

- Uso de algoritmos criptográficos reconhecidos e atualizados conforme normas nacionais e internacionais;
- Proteção contra acesso não autorizado e contra vulnerabilidades conhecidas;
- Conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais normativos de segurança da informação.
- Para os serviços web do MJSP, exigir implantação e manutenção contínua de certificados **SSL/TLS válidos** (cadeia confiável, algoritmo atual, período de validade adequado) e monitoração do **estado de HTTPS** nas aplicações críticas.

5.2.6. Escalabilidade e Continuidade Operacional

5.2.6.1. A solução deve permitir expansão proporcional à demanda, considerando o crescimento estimado de 40% no uso de certificados em relação ao contrato vigente, sem prejuízo à performance ou à segurança.

5.2.6.2. Também deve garantir alta disponibilidade, com mecanismos de contingência para evitar interrupções em serviços críticos.

5.2.7. Alinhamento Estratégico

5.2.7.1. As necessidades tecnológicas aqui descritas constam no Inventário de Necessidades do PDTIC 2024–2027 do MJSP, reforçando o vínculo com as diretrizes estratégicas de transformação digital, modernização e governança de TIC da instituição.

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

6.1. A escolha da solução de certificação digital deve observar os seguintes requisitos adicionais, necessários e suficientes para assegurar o atendimento completo da demanda institucional, em conformidade com a legislação vigente e as boas práticas de governança de TIC:

a) Regularidade institucional:

- A empresa fornecedora deverá estar **credenciada junto à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)** como Autoridade Certificadora (AC) ou atuar em parceria direta com uma AC habilitada, conforme os requisitos definidos pelo Instituto Nacional de Tecnologia da Informação (ITI).

b) Garantia de continuidade:

- A solução deve garantir **continuidade da prestação dos serviços** durante toda a vigência contratual, com capacidade de atender prontamente novas demandas que possam surgir, inclusive em razão de expansão organizacional ou aumento de escopo de sistemas.

c) Prazos e condições de entrega:

- A entrega dos certificados digitais deverá ocorrer **em prazo razoável e previamente estabelecido**, inclusive com critérios diferenciados de urgência para casos críticos ou emergenciais devidamente justificados.

d) Modelo de contratação:

- O modelo de fornecimento poderá ser por **demanda**, mediante controle de consumo mensal ou por cotas anuais, com detalhamento do saldo disponível e gestão facilitada por meio de portal de atendimento e relatórios gerenciais.

e) Capacitação e orientação:

- A contratada deverá prover **material orientativo** e, se necessário, **capacitação técnica básica** aos usuários e gestores sobre o uso, instalação e renovação dos certificados.

f) Conformidade com políticas internas:

- A solução deve estar alinhada à **Política de Segurança da Informação (PSI)** e à **Política de Governança de TIC** do MJSP, respeitando diretrizes de acesso, autenticação, integridade da informação e gestão de ativos.

g) Flexibilidade e escalabilidade:

- A solução contratada deve permitir **ajuste de quantitativos contratados**, respeitando limites e regras do contrato, sem comprometer a qualidade do serviço e o cumprimento do SLA.

6.2. Verificação de enquadramento no Catálogo de Soluções de TIC do SISP

6.2.1. Nos termos do art. 9º, § 6º, da Instrução Normativa SGD/ME nº 94/2022, foi realizada verificação quanto à existência de item correspondente no Catálogo de Soluções de TIC com Condições Padronizadas publicado pelo Órgão Central do SISP.

6.2.2. Após consulta ao referido Catálogo, constatou-se que a solução pretendida — serviços de emissão, renovação e revogação de certificados digitais no padrão ICP-Brasil — não consta como item padronizado com PMC-TIC definido.

6.2.3. Dessa forma, a presente contratação não se submete à utilização obrigatória de elementos padronizados constantes de Catálogo, tais como especificações técnicas, níveis de serviço ou PMC-TIC.

6.2.4. Registra-se que, caso venha a ser publicada solução padronizada aplicável durante a tramitação do processo, será realizada a devida adequação, se cabível.

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A presente contratação tem por objetivo assegurar a continuidade e a ampliação da infraestrutura de certificação digital do Ministério da Justiça e Segurança Pública (MJSP), indispensável à autenticação forte de usuários e sistemas, à assinatura eletrônica com validade jurídica e à proteção de canais de comunicação (HTTPS) em portais, APIs e serviços integrados. O uso de certificados digitais é condição técnica para a operação regular de sistemas estruturantes como SEI, SCDP, SIASG, SICAF, SIAPE/SIGEP,SIAFI, entre outros Sistemas de entidades como a SENAPPEN e ANPD, além de compor a política de segurança da informação do Ministério ao garantir integridade, autenticidade, confidencialidade e não repúdio dos atos praticados em meio eletrônico.

7.2. A estimativa de demanda foi construída sobre base de evidências históricas. Tomou-se como referência o consumo e a execução do Contrato nº 13 /2021 (SERPRO), ainda vigente até março de 2026, as séries históricas (mar/2024–ago/2025), que demonstram uso contínuo e essencial de certificados para pessoas físicas e jurídicas e para a proteção de serviços publicados. Esses registros evidenciam ciclos de renovação, com picos de demanda, e um crescimento consistente do número de domínios e integrações que exigem certificados SSL/TLS válidos.

7.3. As tabelas abaixo demonstram o histórico das demandas de certificação digital no período de abril de 2021 à agosto de 2025:

Volume de Certificados Digitais faturados em 2021-2022							
		Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Certificado digital para Pessoa Física A3, 3 anos, com token	Certificado digital para equipamento A1, 1 ano	Certificado digital para Pessoa Jurídica, 3 anos, sem token	Certificado digital para Pessoa jurídica, 3 anos, com token
Quantidade Contratada		125	250	64	38	13	25
Quantidade Emitida	abr/21	0	0	3	0	0	0
	mai/21	0	0	3	0	0	0
	jun/21	0	0	8	2	0	0
	jul/21	0	0	5	3	0	0
	ago/21	0	0	0	0	0	0
	set/21	0	7	4	0	0	0
	out/21	3	6	2	0	0	0
	nov/21	0	9	1	0	0	0
	dez/21	0	11	1	0	0	0
	jan/22	0	11	2	0	0	0
	fev/22	0	13	7	0	0	0
	mar /22	0	16	2	0	0	0
Quantidade Total Emitida		3	132	38	5	0	0
Saldo		122	118	26	33	13	25

Volume de Certificados Digitais faturados em 2022 - 2023						
	Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Certificado digital para Pessoa Física A3, 3 anos, com token	Certificado digital para equipamento A1, 1 ano	Certificado digital para Pessoa Jurídica, 3 anos, sem token	Certificado digital para Pessoa jurídica, 3 anos, com token
Quantidade Contratada	125	250	64	38	13	25

Quantidade Emitida	mar /22	0	10	0	0	0	0
	abr /22	1	11	4	0	0	0
	mai /22	0	11	2	1	0	0
	jun /22	6	26	1	4	0	0
	jul/22	8	16	3	0	0	0
	ago /22	2	26	9	0	0	0
	set/22	0	13	1	0	0	0
	out /22	4	9	3	0	0	0
	nov /22	0	12	9	0	0	0
	dez /22	1	7	3	0	0	0
	jan/23	1	9	3	0	0	0
	fev /23	0	10	5	0	0	0
	mar /23	2	5	4	0	0	0
Quantidade Total Emitida		25	165	47	5	0	0
Saldo		100	85	17	33	13	25

Volume de Certificados Digitais faturados em 2023 - 2024							
		Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Certificado digital para Pessoa Física A3, 3 anos, com token	Certificado digital para equipamento A1, 1 ano	Certificado digital para Pessoa Jurídica, 3 anos, sem token	Certificado digital para Pessoa jurídica, 3 anos, com token
Quantidade Contratada		125	250	64	38	13	25
Quantidade Emitida	mar/23	0	3	2	0	0	0
	abr/23	0	11	2	0	0	1
	mai/23	0	2	2	1	0	0
	Jun 2023	1	11	5	4	0	0
	jul/23	1	10	4	3	0	1
	ago/23	1	11	3	0	0	0
	set/23	0	5	2	1	0	0
	out/23	0	9	7	0	0	0
	nov/23	20	12	7	0	0	0
	dez/23	8	5	0	2	0	0
	jan/24	5	2	2	0	0	0
	fev/24	1	5	0	0	0	0
	mar/24	1	5	1	0	0	0
Quantidade Total Emitida		38	91	37	11	0	2

Saldo	87	159	27	27	13	23

Volume de Certificados Digitais faturados em 2024 - 2025							
		Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Certificado digital para Pessoa Física A3, 3 anos, com token	Certificado digital para equipamento A1, 1 ano	Certificado digital para Pessoa Jurídica, 3 anos, sem token	Certificado digital para Pessoa jurídica, 3 anos, com token
Quantidade Contratada		125	250	64	38	13	25
Quantidade Emitida	mar /24	0	3	0	0	0	0
	abr /24	3	25	5	0	0	0
	mai /24	5	36	5	5	0	0
	jun /24	6	7	2	1	0	0
	jul /24	5	8	2	1	0	0
	ago /24	11	53	2	0	0	0
	set /24	7	14	1	0	0	0
	out /24	0	14	0	0	0	0
	nov /24	0	10	0	0	0	0
	dez /24	0	12	0	0	0	0
	jan /25	0	10	0	0	0	0
	fev /25	0	17	0	0	0	0
	mar /25	16	10	7	0	0	1
Quantidade Total Emitida		53	219	24	7	0	0
Saldo		72	31	40	31	13	24

Volume de Certificados Digitais faturados em 2025							
		Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Certificado digital para Pessoa Física A3, 3 anos, com token	Certificado digital para equipamento A1, 1 ano	Certificado digital para Pessoa Jurídica, 3 anos, sem token	Certificado digital para Pessoa jurídica, 3 anos, com token
Quantidade Contratada		125	250	64	38	13	25
	mar/25	0	3	2	0	0	0
	abr/25	10	15	4	0	0	0

Quantidade Emitida	mai/25	4	9	2	3	0	0
	jun/25	3	7	3	0	0	0
	jul/25	6	16	7	0	0	0
	ago/25	6	18	10	1	0	0
Quantidade Total Emitida		29	68	28	4	0	0
Saldo		96	182	36	34	13	25

7.4. Além da tendência de expansão do consumo já observada, há fatores recentes que pressionam a demanda e justificam a atualização dos quantitativos. Destaca-se a exigência operacional de uso de certificado digital para autenticação e assinatura de ordens de pagamento no SIAFI, o avanço da transformação digital com eliminação de papel e a ampliação de integrações com plataformas federais acessadas via identidade digital institucional. Esses fatores, somados ao ingresso de novos servidores e à necessidade de resiliência operacional para lidar com janelas concentradas de renovação, exigem dimensionamento prudente e preventivo da capacidade instalada.

7.5. Com base nesse conjunto de elementos, aplicou-se um fator de crescimento de aproximadamente **40% (quarenta por cento)** sobre a média anual de consumo do contrato vigente, considerando: i) novas obrigatoriedades e reforços de segurança que ampliam o público que necessita de certificado; ii) aumento da base de usuários e frentes de trabalho que dependem de acesso autenticado; iii) expansão do parque de serviços e integrações que demandam SSL/TLS adicionais e rotação de chaves; e iv) necessidade de “pulmão” operacional para absorver picos trienais de renovação sem emissões emergenciais. Não se trata, portanto, de uma margem arbitrária, mas da tradução quantitativa de normativos e operacionais observáveis sobre uma base histórica.

7.6. O resultado dessa metodologia está consolidado na tabela de estimativas por item, que contempla a cesta necessária de certificados para o período: e-CPF A3 para pessoa física (em nuvem, com e sem AR, e em token), e-CNPJ A3 para pessoa jurídica e certificados SSL/TLS para aplicações especiais. As quantidades projetadas visam garantir continuidade, absorver o crescimento esperado e reduzir o risco de insuficiência de licenças em momentos críticos, mantendo o nível de serviço exigido pelos sistemas internos e pelos ambientes integrados com outros órgãos.

7.7. Cumpre registrar que os certificados para equipamentos A1 utilizados no contrato anterior foram substituídos por certificados SSL/TLS (aplicações especiais), adequados à proteção de canais HTTPS e à autenticação de servidores e APIs, com maior padronização e melhor governança de ciclo de vida. Quanto aos certificados digitais para Pessoa Jurídica com token, estes foram descontinuados, mantendo-se apenas a emissão sem mídia criptográfica (sem token), por apresentar maior eficiência operacional, menor ônus logístico e plena aderência às integrações e às políticas de segurança vigentes no MJSP.

7.8. Para sustentar a execução com segurança e previsibilidade, a gestão será apoiada por inventário centralizado de certificados, alertas de validade antecipados, acompanhamento de publicação e consulta de CRL/OCSP e relatórios periódicos de volumetria e prazos de emissão, renovação e revogação. Esse arranjo favorece a rastreabilidade, a conformidade com a ICP-Brasil e a aderência à LGPD, além de permitir revisões trimestrais dos quantitativos executados e eventuais realocações entre itens, se necessário, sem perda de padronização e sem ruptura dos níveis de serviço.

7.9. Em síntese, a demanda ora apresentada é robusta porque se ancora no histórico real de consumo, incorpora mudanças normativas e operacionais recentes e materializa, em termos quantitativos, a necessidade de garantir continuidade, regularidade e segurança jurídica das operações do MJSP. O acréscimo de 40% sobre o histórico recente confere a folga operacional necessária para lidar com picos de renovação e expansão de escopo, evitando emissões de urgência, interrupções de sistemas e riscos de não conformidade.

7.10. A seguir, apresenta-se a tabela contendo a estimativa detalhada dos tipos de certificados digitais, com suas respectivas quantidades **projetadas**, conforme parâmetros de mercado e contratações anteriores:

Item	CATMAT / CATSER	Descrição	Qtde.
1	27154	Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	168
2	27251	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	336
3	27189	Certificado digital para Pessoa Física A3, 3 anos, com token	84
4	27170	Certificado SSL/TLS (aplicações especiais)	36

5	27227	Certificado digital para Pessoa Jurídica, 3 anos	12

7.4. Justificativa do Prazo Contratual

7.4.1. Considerando a natureza continuada da certificação digital, sua indispensabilidade para acesso a sistemas estruturantes do Governo Federal e o ciclo de validade dos certificados (até 3 anos), entende-se tecnicamente adequada a contratação com vigência inicial de 36 (trinta e seis) meses.

7.4.2. A adoção de prazo plurianual permite melhor gestão do ciclo de vida dos certificados, mitiga riscos de descontinuidade e reduz custos administrativos associados a processos licitatórios recorrentes, mantendo alinhamento com o planejamento estratégico de TIC do MJSP.

8. Levantamento de soluções

8.1. Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas

8.1.1. Foram realizadas pesquisas no Portal Nacional de Contratações Públicas, por contratações de soluções de digitalização adotados em outros órgãos ou entidades da administração pública. Nos itens abaixo foram listadas contratações com itens semelhantes ao da contratação em estudo.

8.1.1.1. Órgão: **MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES** - UASG: 240127

- Contratação Direta nº 57/2025 - Processo Administrativo nº : 01207.000254/2025-31
- Data do Contrato: 17/07/2025
- Endereço: https://pncp.gov.br/app/editais/01263896000164/2025/500
- Contratação junto ao SERPRO

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Emissão de Certificado Digital A3, sem Token Pessoa Física	20	R$ 169,47	R$ 3.389,40
2	Emissão de Certificado Digital A3, sem Token Pessoa Física	10	R$ 194,06	R$ 1.940,60
3	Emissão de Certificado Digital A3, sem Token Pessoa Jurídica	5	R$ 284,49	R$ 1.422,45

8.1.1.2. Órgão: **INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DO MARANHAO** - UASG:158128

- Contratação Direta nº 8/2025 - Processo Administrativo nº : 23249.019772/2025-74
- Data do Contrato: 07/08/2025
- Endereço: https://pncp.gov.br/app/editais/10735145000194/2025/118
- Contratação junto ao SERPRO

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Emissão de Certificado Digital A3, com Token Pessoa Física	30	R$ 63,12	R$ 1.893,60
2	Emissão de Certificado Digital A3, sem Token Pessoa Física	50	R$ 34,86	R$ 1.743,00
3	Emissão de Certificado Digital A3, Nuvem, Pessoa Física	250	R$ 75,27	R$ 18.817,50
4	Emissão de Certificado Digital A3, com Token Pessoa Jurídica	5	R$ 331,59	R$ 1.657,95

5	Emissão de Certificado Digital A3, Nuvem Pessoa Jurídica	30	R$ 235,41	R$ 7.062,30
6	Certificado SSL - ICP-Brasil	6	R$ 1.181,30	R$ 7.087,80

8.1.1.3. Órgão: **ADVOCACIA GERAL DA UNIAO- DIRETORIA DE LOGISTICA E GESTÃO DOCUMENTAL** - UASG:110792

- Contratação Direta nº 71/2025 - Processo Administrativo nº : 00693.000715/2025-78
- Data do Contrato: 26/08/2025
- Endereço: https://pncp.gov.br/app/editais/26994558000123/2025/133
- Contratação junto ao SERPRO

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	CERTIFICADO DIGITAL COM IMUNIDADE VAREJO PF E PJ (3 ANOS) SERPRO ID EMISSÃO VIA MÓDULO	3065	R$75,27	R$230.702,55
2	CERTIFICADO DIGITAL COM IMUNIDADE VAREJO PJ AE (3 ANOS)	3065	R$34,86	R$106.845,90
3	CERTIFICADO DIGITAL COM IMUNIDADE VAREJO PJ A3 (3 ANOS) COM TOKEN	3065	R$63,12	R$193.462,80
4	CERTIFICADO DIGITAL COM IMUNIDADE VAREJO EQUIPAMENTO A1 (1 ANO)	2	R$1.181,30	R$2.362,60
5	CERTIFICADO DIGITAL COM IMUNIDADE VAREJO EQUIPAMENTO MULTIDOMÍNIO A1 (1 ANO)	2	R$2.967,39	R$5.934,78

8.2. As alternativas do mercado

8.2.1. No mercado brasileiro há Autoridades Certificadoras (ACs) privadas, credenciadas na ICP-Brasil, que fornecem diversos tipos de certificados: certificados para pessoa física (e-CPF A3), pessoa jurídica (e-CNPJ A3) e certificados SSL/TLS para sites, portais e APIs.

8.2.2. O que essas empresas oferecem (em linhas gerais):

8.2.2.1. Tipos de certificado: e-CPF A3 e e-CNPJ A3 com validade de até 3 anos, em duas formas:

- Em nuvem (sem token), com autenticação forte (ex.: MFA) e uso em computador e celular;
- Com token/smartcard (mídia física), quando o órgão preferir;
- SSL/TLS para aplicações: domínio único, multidomínio (SAN) e wildcard, com suporte a TLS 1.2/1.3 e chaves RSA/ECDSA, para proteger HTTPS de portais e integrações;
- Atendimento e validação: rede de Autoridades de Registro (AR) para validar identidade presencialmente e, quando previsto, por videoconferência;
- Gestão do ciclo de vida: portal e/ou API para a TI do órgão emitir, renovar e revogar; inventário dos certificados, alertas de vencimento (ex.: 60 /30/15 dias) e relatórios;
- Status e revogação: publicação e consulta de CRL/OCSP (listas e respostas online que dizem se o certificado segue válido);
- Suporte e SLA: canais de atendimento (usuário e TI) com acordos de nível de serviço para prazos de emissão, renovação e disponibilidade dos serviços;
- Conformidade: credenciamento no ITI/ICP-Brasil, PC/DPC publicadas, auditorias periódicas e adequação à LGPD;
- Integrações: guias de configuração para SEI, SIAFI, portais e APIs, servidores web e pipelines (CI/CD), inclusive exemplos de CSR, instalação e rotação de chaves;
- Modelos de contratação: por unidade, por pacote ou por assinatura/franquia (mensal/anual), conforme o volume do órgão;

- Sustentabilidade: uso em nuvem reduz deslocamentos e dispensa mídias físicas (tokens), diminuindo logística e descarte.

8.2.2.2. Governança típica oferecida:

- Definição de papéis e responsabilidades (órgão x fornecedor), comunicação de janelas e incidentes, indicadores (disponibilidade de CRL/OCSP, tempo de emissão, taxa de sucesso) e relatórios periódicos para acompanhamento e fiscalização do contrato.

8.2.3. Esse é o “pacote padrão” encontrado nas ACs privadas do mercado, cobrindo as necessidades de e-CPF/e-CNPJ A3 e SSL/TLS com ferramentas de gestão, suporte e conformidade que o MJSP precisa para operar com segurança e previsibilidade.

8.3. Existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações

Não se aplica.

8.4. Políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis

8.4.1. Esta contratação observará, no que couber, os padrões federais:

- ICP-Brasil: aplicável integralmente (é o núcleo do objeto). A contratada deve cumprir as normas do ITI (PC/DPC, cadeia de certificação completa, emissão/renovação/revogação, e disponibilidade de CRL/OCSP com SLA).

- ePING (interoperabilidade): aplicável para uso de protocolos e formatos abertos/seguros (p.ex., X.509 v3, TLS 1.2/1.3) e documentação dos endpoints (OCSP/CRL e APIs de gestão do ciclo de vida).

- eMAG (acessibilidade): aplicável quando houver interfaces/portais fornecidos ao MJSP. As telas devem seguir requisitos de acessibilidade equivalentes a WCAG 2.1 nível AA.

- ePWG e Design System de Governo (DSGov): aplicáveis às interfaces sob domínio do MJSP/gov.br. Se houver páginas/embeds nesses ambientes, devem seguir os padrões web e o DSGov. Portais próprios do fornecedor devem, no mínimo, adotar boas práticas web (responsividade, segurança).

- e-ARQ Brasil (gestão arquivística): aplicável aos sistemas do MJSP que guardam documentos assinados. A contratada deve garantir a verificabilidade ao longo do tempo (cadeia confiável disponível, CRL/OCSP acessíveis e documentação para validação).

8.5. Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual

8.5.1. De modo geral, não são necessárias obras, aquisição de hardware dedicado ou ampliações relevantes de datacenter para a execução contratual.

8.6. Diferentes modelos de prestação do serviço

8.6.1. As possibilidades são abordadas no item 9 - ANÁLISE COMPARATIVA DAS SOLUÇÕES

8.7. Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes

8.7.1. Os serviços de certificação podem ser prestados em diferentes modelos. No formato on-demand, as emissões e renovações são feitas por unidade, conforme a necessidade do órgão, com preço unitário por certificado. Há também o modelo por pacotes ou lotes, no qual se adquire previamente uma quantidade por perfil (e-CPF, e-CNPJ, SSL/TLS) e se consome ao longo da vigência. Alternativamente, é possível contratar por assinatura ou franquia, definindo um volume mensal ou anual de emissões, geralmente com ferramentas de gestão incluídas.

8.7.2. Em todos os modelos, o fornecedor pode ofertar serviço gerenciado de ciclo de vida, cuidando do inventário de certificados, alertas de vencimento, renovações programadas, trilhas de auditoria, relatórios e procedimentos de continuidade. A validação de identidade (AR) ocorre presencialmente nos postos da AC e, quando previsto em política, por videoconferência, com registros e evidências adequadas.

8.7.3. Para os certificados de pessoa (e-CPF/e-CNPJ A3), o uso pode ser em nuvem — sem mídia física, com autenticação forte e mobilidade — ou com token/smartcard quando o processo de negócio exigir. No caso de SSL/TLS para aplicações, o catálogo usual contempla domínio único, multidomínio (SAN) e wildcard, com suporte a TLS 1.2/1.3 e possibilidade de automação de emissão/renovação via portal ou API.

8.7.4. As integrações costumam incluir portal e/ou API administrativa para a equipe de TI solicitar, aprovar e acompanhar emissões; publicação e consulta de CRL/OCSP; e relatórios operacionais e gerenciais. Os contratos normalmente preveem SLA para prazos de emissão, renovação e disponibilidade dos serviços, além de canais de suporte em níveis.

8.7.5. Quanto ao faturamento, é comum a contratação por unidade, por pacote/lote ou por assinatura/franquia. Itens acessórios, como mídias (token) e validação por videoconferência, quando existentes, podem ter precificação específica.

8.8. Possibilidade de aquisição na forma de bens ou contratação como serviço

8.8.1. As possibilidades são abordadas no item 9 - ANÁLISE COMPARATIVA DAS SOLUÇÕES.

8.9. Ampliação ou substituição da solução implantada

8.9.1. As possibilidades são abordadas no item 9 - ANÁLISE COMPARATIVA DAS SOLUÇÕES.

8.10. Diferentes métricas de prestação do serviço e de pagamento

8.10.1. A métrica de prestação de serviço será baseada na emissão de ordem de serviço para definição do volume inicial necessário ao atendimento das demandas do órgão, com pagamento com periodicidade mensal pelos serviços utilizados. Havendo necessidade de expansão , será realizada nova ordem de serviço com os quantitativos adicionais.

8.11. Levantamento de soluções

8.11.1. De acordo com o objeto da contratação, foram mapeados as seguintes possíveis soluções para a contratação:

Alternativa	Descrição
Solução 1 – SERPRO (reuso de solução pública)	Contratação direta de Autoridade Certificadora pública integrante da ICP-Brasil.
Solução 2 – ACs privadas (mercado ICP-Brasil)	Licitação para contratar Autoridade Certificadora privada credenciada no ITI/ICP-Brasil.
Solução 3 – Execução interna (in house)	Implantação e operação, pelo MJSP, de infraestrutura própria de certificação (AC/AR) aderente à ICP-Brasil.

9. Análise comparativa de soluções

9.1. Para atender à necessidade institucional de emissão de certificados digitais do Ministério da Justiça e Segurança Pública (MJSP), foram analisadas as seguintes alternativas de soluções tecnológicas disponíveis no mercado:

9.1.1. SOLUÇÃO 1: Contratação direta junto ao SERPRO. O Serviço Federal de Processamento de Dados (SERPRO), empresa pública vinculada ao Ministério da Fazenda e Autoridade Certificadora integrante da ICP-Brasil, é o atual fornecedor de certificados digitais do MJSP, com vigência contratual até março de 2026 (Contrato nº 13/2021). Nessa alternativa, a contratação é estruturada com base na dispensa de licitação prevista no art. 75, inciso IX, da Lei nº 14.133/2021, observada a compatibilidade de preços com o mercado. O escopo típico abrange emissão e renovação de certificados e-CPF e e-CNPJ (A3, em token e/ou em nuvem, conforme catálogo), certificados SSL/TLS para aplicações especiais, além da operação de Autoridade de Registro (AR) com validação presencial e/ou por videoconferência. A solução compreende ainda integração com plataformas e sistemas governamentais (por exemplo, Gov.br/SIGEPE, SIAFI, SEI), gestão do ciclo de vida (emissão, renovação, revogação), publicação de CRL/OCSP e atendimento aos padrões e políticas do ITI/ICP-Brasil e à LGPD.

9.1.2. SOLUÇÃO 2: Contratação de autoridades certificadoras privadas. Nesta alternativa, o MJSP realiza procedimento licitatório para aquisição de certificados emitidos por Autoridades Certificadoras (ACs) privadas credenciadas no ITI/ICP-Brasil, contemplando perfis e-CPF e e-CNPJ (A3 com token e/ou em nuvem, conforme catálogo do fornecedor), e certificados SSL/TLS para aplicações institucionais. O fornecimento inclui a operação de AR (atendimento presencial e/ou por videoconferência), documentação técnica, suporte e demais serviços correlatos, devendo o edital/contrato estabelecer as condições de conformidade ICP-Brasil, requisitos de segurança da informação e proteção de dados (LGPD), parâmetros de integração com sistemas do MJSP (como SIAFI, SEI, portais e APIs), bem como os acordos de nível de serviço para emissão, renovação, revogação e disponibilidade de CRL/OCSP, além de mecanismos de gestão do ciclo de vida dos certificados (inventário, monitoramento de validade e trilhas de auditoria).

9.1.3. SOLUÇÃO 3: Execução interna por equipe própria (in house). Esta alternativa consiste na implantação e operação, pelo próprio MJSP, de uma infraestrutura completa de certificação, envolvendo provisionamento de módulos de segurança criptográfica (HSM), ambientes de produção e contingência com requisitos físicos e lógicos de segurança (incluindo sala-cofre ou equivalente), serviços de publicação e consulta de revogação (CRL /OCSP), estabelecimento de Autoridade de Registro com fluxos de validação presencial e/ou por videoconferência, definição de políticas e práticas de certificação aderentes à ICP-Brasil, realização de auditorias periódicas, manutenção de registros e monitoramento contínuo. Implica, ainda, na constituição de equipe dedicada para a operação 24×7, suporte aos usuários, integração com os sistemas internos (como SIAFI, SEI, portais institucionais e APIs) e governança do ciclo de vida dos certificados, incluindo processos de emissão, renovação e revogação, guarda de chaves e rotação conforme políticas internas e normativos aplicáveis.

9.1.4. O quadro a seguir consolida as principais alternativas de fornecedores e tipos de certificados digitais utilizados, com destaque para a solução atualmente adotada pelo MJSP e outras opções levantadas, considerando requisitos de conformidade com a ICP-Brasil e vantajosidade administrativa:

Alternativas de Soluções	**SOLUÇÃO 1:** **Contratação direta junto ao SERPRO**	**SOLUÇÃO 2:** **Aquisição junto a Autoridades Certificadoras Privadas**	**SOLUÇÃO 3:** **Execução Interna (in house)**
Continuidade / Tempo de Implantação	Alta / Curto (serviço já disponível).	Média / Médio (processo licitatório + homologações)	Baixa / Longo (projeto, credenciamento, auditorias e operação).
Viabilidade técnica	Alta. Solução já utilizada e plenamente integrada aos sistemas do MJSP, com suporte técnico e conformidade com a ICP-Brasil.	Alta. Empresas privadas também seguem os padrões ICP-Brasil. Exige integração e migração, além de análise de compatibilidade.	Baixa. Para atender à ICP-Brasil, seria necessário credenciamento no ITI e operar toda a infraestrutura crítica (HSM, sala-cofre, CRL/OCSP, auditorias, equipe 24×7), com alta complexidade técnica. O CAPEX/OPEX e o prazo de implantação seriam elevados, aumentando o risco de não conformidade e de indisponibilidade para sistemas críticos.
Viabilidade jurídica	Alta. Permite contratação direta com base no Art. 75, IX da Lei nº 14.133 /2021, por se tratar de entidade integrante da Administração Pública.	Alta. Exige licitação, salvo exceções legais. Pode-se adotar pregão eletrônico para contratação.	É viável se o MJSP se credenciar no ITI (ICP-Brasil) como AC/AR, observando a MP 2.200-2/2001 e os DOC-ICP (PC/PS, auditorias etc.).
Conformidade com a ICP-Brasil	Plena. Certificados emitidos com padrão ICP-Brasil, inclusive com infraestrutura validada e reconhecida legalmente.	Plena. Desde que a empresa seja certificadora reconhecida pela ICP-Brasil, mantém plena conformidade.	Exige credenciamento no ITI e atendimento integral aos DOC-ICP (PC/PS), com segurança física e lógica, HSM homologado, cerimônias de chaves, operação de AR, CRL /OCSP e auditorias periódicas.
Riscos operacionais	Baixos. Continuidade assegurada, compatibilidade técnica e menor curva de aprendizado.	Médios. Necessidade de novos contratos, capacitação de usuários e eventuais ajustes sistêmicos.	Elevado: dependência de equipe especializada 24×7, gestão de HSM/sala-cofre, CRL/OCSP e cerimônias de chaves, com pontos únicos de falha e alta complexidade de continuidade/DR. Falhas de conformidade ICP-Brasil/ITI ou indisponibilidade afetariam sistemas críticos, gerando paralisações, revogações emergenciais e exposição a incidentes de segurança.
Estimativa de Custo	Compatível com o mercado e com histórico contratual vigente.	Variável - Pode ser inferior, mas exige gestão e logística adicional.	Indefinido - Depende de fornecedores e não cobre todas as necessidades. Maior consumo de infraestrutura própria (energia /refrigeração).
Prazo de Implantação	Curto(serviço já disponível)	Médio (processo licitatório + homologações	Longo (projeto, credenciamento, auditorias e operações)
Suporte/SLA	Atendimento a usuário e TI; ANS para emissão/renovação/OCSP/CRL.	Atendimento conforme contrato; ANS definidos em edital.	Equipe interna 24×7 ou conforme desenho organizacional.
Escalabilidade	Alta (economias de escala do serviço público).	Alta (depende do fornecedor e do contrato)	Condicionada à capacidade interna e investimentos.

10. Registro de soluções consideradas inviáveis

10.1. Solução 2 - Contratação de ACs privadas (inviável):

10.1.1. A adoção dessa alternativa exigiria procedimento licitatório, com fases de disputa, homologação e mobilização do(s) fornecedor(es), além de *cutover* técnico e operacional. Esse ciclo não se compatibiliza com a necessidade de continuidade imediata dos serviços críticos (p.ex., autenticação

/assinatura em SIAFI e SEI), pois introduz janela de transição, ajustes de integração, testes de aceite e treinamento de usuários/AR, ampliando o risco de interrupções e de degradação de serviço em período sensível.

10.1.2. Do ponto de vista técnico, seria necessário replicar integralmente os perfis hoje utilizados no MJSP, incluindo A3 em nuvem com validade de 3 anos e validação remota por vídeo (sem AR presencial), fluxos de emissão/renovação e integrações já consolidadas. O mercado privado apresenta heterogeneidade de políticas de certificação, cadeias de confiança, métodos de validação remota, aplicações de uso e requisitos de dispositivos, sem evidência de equivalência homogênea e comprovada, no escopo e prazo desta contratação. Essa assimetria impede o fracionamento do objeto em bases técnicas uniformes e dificulta a manutenção de um arranjo único e padronizado de identidade digital institucional.

10.1.3. Há, ainda, impactos relevantes de governança e logística: multiplicidade de contratos, SLAs, portais e ARs; necessidade de gerir tokens/mídias quando aplicável; e distribuição em larga escala para matriz, cerca de 90 CNPJs de filiais e fundos. Isso eleva a complexidade de inventário de certificados, monitoramento de validade, revogação, auditoria e trilhas de conformidade, com reflexo direto na rastreabilidade e na gestão do risco operacional.

10.1.4. Por fim, a alternativa demandaria readequação de governança, integrações e ANSs, além de incorrer em riscos licitatórios (eventual deserto /fracasso, impugnações, recursos) e de transição. Consideradas essas condicionantes — continuidade, equivalência técnica, padronização, logística e governança — a contratação de ACs privadas é registrada como inviável para o escopo e horizonte temporal desta contratação, sem prejuízo de futura reavaliação em outro ciclo de planejamento.

10.2. Solução 3 - Execução interna por equipe própria (in house) (inviável):

10.2.1. A implantação de uma solução interna exigiria que o MJSP estruturasse e operasse, sob sua responsabilidade direta, toda a cadeia de certificação com validade jurídica na ICP-Brasil. Isso implica, no mínimo, submeter-se ao processo de credenciamento junto ao ITI, elaborar e manter Políticas de Certificação (PC) e Declarações de Práticas de Certificação (DPC/PS), instituir Autoridade Certificadora (AC) e Autoridade de Registro (AR) com segregação de funções (gestão, operação, segurança e auditoria), e comprovar controles físicos e lógicos aderentes aos DOC-ICP. Do ponto de vista de infraestrutura, seriam necessários HSMs redundantes para geração e guarda de chaves-raiz e operacionais, ambientes de produção e contingência com alta disponibilidade, publicação e atendimento de CRL/OCSP, repositórios confiáveis (HTTP/LDAP), cerimônias de chaves documentadas e auditáveis, sala-cofre (ou equivalente) com requisitos de proteção e monitoramento, além de processos de gestão de incidentes, continuidade de negócios e testes de recuperação de desastres.

10.2.2. Operacionalmente, a solução demandaria equipe especializada 24×7 para operação de AC/AR, suporte a usuários, manutenção de repositórios e validações, execução de auditorias periódicas independentes, atendimento a fiscalizações, rotação de chaves e atualização contínua de componentes criptográficos e procedimentos. Também recairiam sobre o órgão as responsabilidades por trilhas de auditoria imutáveis, registro e retenção de logs, gestão de riscos, conformidade à LGPD, hardening, revisão de acessos, e atualização tempestiva de algoritmos e tamanhos de chaves, sob pena de comprometer a cadeia de confiança. Em termos de custos e prazos, o CAPEX (HSMs, ambientes, segurança física, ferramentas) e o OPEX (pessoal, auditorias, manutenção, suporte e continuidade) são elevados e recorrentes, com prazo de implantação prolongado e alto risco de não conformidade ou indisponibilidade impactando diretamente sistemas estruturantes (como SIAFI e SEI). Diante desse conjunto de requisitos regulatórios, técnicos e operacionais, a execução interna não atende ao horizonte temporal nem às condições de continuidade e governança requeridas nesta contratação, sendo, portanto, registrada como inviável para o escopo em análise.

11. Análise comparativa de custos (TCO)

11.1. Nos termos do **art. 11, inciso III, da IN SGD/ME nº 94/2022**, a análise de TCO deve considerar **apenas as soluções técnica e funcionalmente viáveis**. No presente caso, após o levantamento e a avaliação de viabilidade, **remanescem viáveis apenas os serviços de certificação digital providos pelo SERPRO**, razão pela qual **não se aplica** a comparação de custos entre alternativas. As demais soluções identificadas foram registradas neste ETP como **inviáveis**, para fins de transparência e controle.

11.2. Dessa forma, apresenta-se **exclusivamente** o TCO da solução viável, calculado com base na **cesta homogênea de itens e quantitativos estimados** neste ETP, considerando **preços unitários**, **eventuais serviços acessórios** (AR, suporte/SLA), **vigência e reajustes**, bem como a **distribuição anual do desembolso** durante o período contratual, em consonância com a definição e finalidade do **ETP** estabelecida na **Lei nº 14.133/2021**.

12. Descrição da solução de TIC a ser contratada

12.1. A solução consiste na **contratação direta do SERPRO** para o provimento de serviços de **certificação digital aderentes à ICP-Brasil**, com **gestão centralizada do ciclo de vida** dos certificados utilizados pelo Ministério da Justiça e Segurança Pública (MJSP). O escopo cobre emissão, renovação, revogação, suporte e integração com sistemas corporativos e estruturantes, observando requisitos técnicos, legais e de segurança da informação.

12.1.1. Escopo funcional

- **Certificados para pessoas físicas (e-CPF A3):** emissão em **token** e em **nuvem** (*A3 em nuvem do SERPRO – SerproID*), com validade de até 3 anos, para autenticação e assinatura digital de atos e documentos oficiais.

- **Certificados para pessoas jurídicas (e-CNPJ A3):** para a unidade matriz do MJSP, **unidades filiais** e **fundos vinculados**, viabilizando acesso a sistemas federais/estaduais/municipais, outorga de procurações eletrônicas e transações fiscais.

- **Certificados A1 (máquina/serviço):** destinados à autenticação de serviços e integrações internas (APIs, serviços de backend e automações), quando aplicável.

- **Certificados SSL/TLS (aplicações especiais):** para proteção de portais, sítios e interfaces de integração do MJSP (HTTPS), garantindo confidencialidade e integridade em trânsito.

12.1.2. Serviços incluídos

- **Operação de Autoridade de Registro (AR):** validação **presencial** e por **videoconferência**, conforme o perfil; coleta e checagem documental; emissão/renovação; orientação ao usuário.

- **Gestão do ciclo de vida:** inventário unificado, alertas de validade, processos de **revogação**, publicação/consulta de **CRL/OCSP**, trilhas de auditoria.

- **Suporte técnico:** atendimento ao usuário e à equipe de TI do MJSP, com **SLA/ANS definidos** (emissão, renovação, revogação, disponibilidade de OCSP/CRL e tempos de resposta).

- **Integração:** compatibilidade com **SIAFI, SEI, SIAPE/SIGEP, Compras.gov.br** e sistemas internos (portais e APIs), incluindo orientações técnicas e, quando necessário, assistência à configuração.

- **Relatórios e auditoria:** relatórios periódicos de emissões, renovações, revogações, incidentes e conformidade; evidências para auditorias internas/externas.

12.1.3. Requisitos técnicos e de segurança

- **Conformidade ICP-Brasil/ITI** (MP 2.200-2/2001 e DOC-ICP): políticas e práticas de certificação, cadeia de confiança, uso de **HSM** pelo prestador, cerimônias de chaves e segregação de funções.

- **Segurança da informação e LGPD:** proteção de dados pessoais, controles de acesso, registro de eventos, guarda segura de chaves e *hardening* dos componentes.

- **Criptografia e padrões:** algoritmos e tamanhos de chave atualizados; certificados **SSL/TLS** com cadeias confiáveis e boas práticas (renovação tempestiva, monitoramento de expiração).

- **Alta disponibilidade e continuidade:** infraestrutura redundante para emissões e serviços de validação (OCSP/CRL), com planos de contingência e testes periódicos.

12.1.4. Governança e papéis

- **SERPRO:** emissão, AR, suporte, operação de OCSP/CRL, manutenção da conformidade ICP-Brasil, relatórios e auditorias.

- **MJSP (gestão do contrato):** definição de perfis (PF/PJ/A1/SSL), autorização de emissões, governança de inventário, aprovação de revogações, fiscalização dos ANS/SLA e do plano de continuidade.

12.1.5. Níveis de serviço (macro-requisitos para o contrato)

- **Prazos máximos** para emissão/renovação por tipo de certificado (PF, PJ, A1 e SSL/TLS).

- **Disponibilidade** de serviços críticos (OCSP/CRL, portal de gestão) com metas mensais/anuais.

- **Suporte:** janelas de atendimento, tempos de resposta/solução por severidade, inclusive **24×7** quando houver impacto em serviços essenciais (ex.: pagamentos no SIAFI).

- **Qualidade:** taxa de êxito em emissões/renovações, tempo médio de validação (AR presencial/vídeo), indicadores de satisfação.

12.1.6. Escalabilidade e planejamento

- Capacidade para **absorver crescimento projetado (~30%)** no período contratual, com elásticos de quantitativos e incremento proporcional de suporte/AR.

- Procedimentos para **onboarding/offboarding** de usuários e unidades (matriz, filiais e fundos), garantindo padronização e rastreabilidade.

12.1.7. Entregáveis e documentação

- Catálogo de serviços e **runbooks** operacionais (emissão/renovação/revogação).
- **Matriz de perfis** (PF/PJ/A1/SSL) e parametrizações (validade, mídias, fluxo AR).
- Relatórios periódicos (inventário, validade, incidentes, ANS/SLA).
- Evidências de conformidade **ICP-Brasil/ITI** e **LGPD**.

13. Estimativa de custo total da contratação

Valor (R$): 158.037,12

13.1. A estimativa total desta contratação, é de **R$ 158.037,12** (**cento e cinquenta e oito mil e trinta e sete reais e doze centavos**).

Item	CATMAT / CATSER	Descrição	Métrica	Qtde.	Valor Unitário	Valor Total
1	27154	Certificado digital para Pessoa Física, 3 anos, em nuvem, com AR	Unidade	168	R$ 179,90	R$ 30.223,20
2	27251	Certificado digital para Pessoa Física, 3 anos, em nuvem, sem AR	Unidade	336	R$ 169,47	R$ 56.941,92
3	27189	Certificado digital para Pessoa Física A3, 3 anos, com token	Unidade	84	R$ 256,00	R$ 21.504,00
4	27170	Certificado SSL/TLS (aplicações especiais)	Unidade	36	R$ 1.254,00	R$ 45.144,00
5	27227	Certificado digital para Pessoa Jurídica, 3 anos	Unidade	12	R$ 352,00	R$ 4.224,00
TOTAL:						**R$ 158.037,12**

14. Justificativa técnica da escolha da solução

14.1. A escolha da solução baseada na contratação de certificados digitais junto ao Serviço Federal de Processamento de Dados (SERPRO), entidade integrante da Administração Pública Federal, encontra respaldo técnico, legal e estratégico para atendimento das necessidades do Ministério da Justiça e Segurança Pública (MJSP).

14.2. A certificação digital é fundamental para garantir a autenticidade, integridade, confidencialidade e não repúdio das transações eletrônicas realizadas por servidores, sistemas e aplicações do MJSP, permitindo o acesso seguro a plataformas como SEI, SIAFI, SIGEPE, Comprasnet, Gov.br, entre outras. Diante disso, a solução adotada contempla diferentes modalidades de certificados — Pessoa Física (com e sem AR), Pessoa Jurídica, selos eletrônicos e certificados de aplicações específicas (AE-S) — compatíveis com os requisitos operacionais do Ministério.

14.3. A contratação da SERPRO se justifica pela natureza pública da entidade, sua larga experiência em serviços de certificação digital em conformidade com o padrão ICP-Brasil e sua capacidade de integração com os sistemas governamentais já utilizados pelo MJSP. A relação direta com a SERPRO também assegura maior controle institucional sobre a gestão dos certificados, facilita o suporte técnico, e permite contratações mais ágeis por meio de dispensa de licitação, conforme o inciso IX do art. 75 da Lei nº 14.133/2021, respeitada a vantajosidade da proposta.

14.4. Além disso, determinadas soluções ofertadas pela SERPRO, como os certificados digitais em nuvem (SerproID), são disponibilizadas com exclusividade para órgãos federais, promovendo economia de escala, padronização e maior eficiência administrativa. Tais soluções atendem integralmente aos critérios de segurança da informação e interoperabilidade com os sistemas da Administração Pública.

14.5. Portanto, a solução de TIC baseada no fornecimento de certificados digitais pelo SERPRO atende de forma técnica, econômica e operacional à totalidade das necessidades institucionais do MJSP, representando a alternativa mais adequada para assegurar a continuidade dos serviços, a conformidade regulatória e a governança digital.

14.6. Do parcelamento da contratação decorrente de aspectos técnicos

14.6.1. O ETP deve justificar o parcelamento ou não do objeto (art. 18, §1º, VIII, da Lei nº 14.133/2021) e observar o princípio do parcelamento quando tecnicamente viável e economicamente vantajoso (art. 47, II, para serviços), ponderando responsabilidade técnica, custos de gestão de múltiplos contratos e ampliação da competição.

14.6.2. Padronização e continuidade como diretriz. A manutenção de cadeia de confiança homogênea, processos unificados de AR (presencial/vídeo), SLA/ANS únicos e métricas consolidadas reduz falhas, evita dispersão de responsabilidades e minimiza a janela de transição sobre serviços críticos. A fragmentação entre fornecedores diferentes eleva o risco de heterogeneidade (políticas/fluxos distintos), dificulta rastreabilidade e aumenta o custo de gestão (múltiplos contratos, integrações e auditorias), incidindo nas ressalvas do art. 40, §3º, notadamente por economia de escala e redução de custos de gestão.

14.6.3. Diretriz para o modelo de contratação. À luz dos critérios técnicos acima e das integrações vigentes, não se recomenda o parcelamento por múltiplos fornecedores. Adota-se um único contrato com itens funcionais internos (e-CPF A3, e-CNPJ A3 e SSL/TLS), preservando competição interna por item quando cabível e mantendo padronização e governança centralizada. A solução SERPRO atende ao arranjo técnico-operacional exigido, com interoperabilidade no ecossistema federal e capacidade de escala nacional, atendendo ao requisito legal de que o parcelamento só deve ocorrer quando tecnicamente viável e economicamente vantajoso.

14.7. Conclusão técnica: Para o presente escopo, **o não parcelamento entre fornecedores** é a opção **mais segura e eficiente**, pois: (i) **assegura continuidade** dos serviços estruturantes; (ii) **preserva a padronização** da identidade digital e dos canais; (iii) **reduz o custo de coordenação** e o risco operacional; e (iv) **atende ao marco legal** (arts. 18, §1º, VIII; 47, II; e 40, V, "b" e §3º, Lei nº 14.133/2021).

15. Justificativa econômica da escolha da solução

15.1. A escolha pela contratação do Serviço Federal de Processamento de Dados (SERPRO) para o fornecimento de certificados digitais atende ao princípio da economicidade e demonstra-se vantajosa sob a ótica financeira e administrativa.

15.2. Trata-se de uma solução pública consolidada, amplamente adotada por diversos órgãos da Administração Pública Federal, o que proporciona condições comerciais competitivas e aderentes ao mercado. Os valores praticados pelo SERPRO foram levantados e comparados a preços médios obtidos por outras instituições, apresentando-se, em muitos casos, inferiores ou equivalentes aos ofertados por Autoridades Certificadoras privadas, com a vantagem adicional de não gerar custos indiretos relacionados à compatibilidade de sistemas, suporte técnico, adaptação de infraestrutura e interoperabilidade.

15.3. A adoção de uma contratação unificada com a SERPRO também reduz os custos administrativos e operacionais, eliminando a necessidade de múltiplos contratos com diferentes fornecedores, simplificando a gestão contratual e garantindo uniformidade nos serviços prestados. Além disso, a possibilidade de contratação plurianual, como já praticado por outros órgãos, evita a descontinuidade do serviço e reduz o esforço de renovações frequentes, gerando economia de escala.

15.4. A opção pelo SERPRO permite ainda explorar soluções tecnológicas específicas, como certificados em nuvem (SerproID), que agregam valor ao processo sem custo adicional para armazenamento físico (tokens ou smartcards), além de facilitarem o uso remoto e a mobilidade, otimizando a atuação dos servidores públicos.

15.5. Dessa forma, a contratação da solução por meio do SERPRO mostra-se a mais vantajosa economicamente para o Ministério da Justiça e Segurança Pública, tanto pelo custo direto dos certificados quanto pela redução de despesas acessórias e pela racionalização da execução contratual, respeitando os princípios previstos nos arts. 11 e 18 da Lei nº 14.133/2021.

15.6. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

15.6.1. O objeto da pretendida contratação, que forma o conjunto de serviços a serem contratados, configura uma Única solução de Tecnologia da Informação.

15.6.2. O grupo abarcou todos os elementos necessários para prover um único Serviço Técnico Especializado de Operação de Infraestrutura e Atendimento a Usuários de Tecnologia da Informação e Comunicação - TIC. Os itens que compõem o grupo representam os elementos necessários que em conjunto formam uma Única solução.

15.6.3. Considerando a dependência entre os itens que compõem o objeto desta contratação, comprovou-se economicamente inviável seu parcelamento, visto que a divisão do objeto pode comprometer o cumprimento dos requisitos técnicos apresentados neste artefato.

15.6.4. A contratação por grupo poderia causar prejuízo para a economia de escala, e tornaria inviável e prejudicial o bom desempenho da contratação, por se tratar de serviços complementares e indissociáveis.

15.6.5. A viabilidade econômica significa que o parcelamento deve trazer benefícios para a Administração, proporcionando um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala ao se contratar o serviço em único lote.

15.6.6. Nesse sentido, a opção do MJSP, em respeito à legislação vigente e na busca pela economicidade e na melhor forma de prestar os serviços, inclusive no que tange à garantia da padronização dos serviços, opta por contratar a solução por meio de um único prestador dos serviços.

16. Benefícios a serem alcançados com a contratação

16.1. Os benefícios esperados para a contratação são:

- **Continuidade dos serviços críticos**: manutenção ininterrupta de acessos e assinaturas digitais em sistemas estruturantes (ex.: SIAFI, SEI), evitando paralisações operacionais e riscos à execução orçamentária e administrativa.
- **Conformidade legal e normativa**: aderência à ICP-Brasil (MP nº 2.200-2/2001), à Lei nº 14.063/2020 (assinaturas eletrônicas), à LGPD e às diretrizes da IN SGD/ME nº 94/2022, assegurando validade jurídica e governança.
- **Segurança da informação reforçada**: garantia de autenticidade, integridade, confidencialidade e não repúdio nas transações eletrônicas, com cadeias de confiança e serviços de OCSP/CRL operando sob SLA.
- **Padronização e governança centralizada**: gestão unificada do ciclo de vida (emissão, renovação, revogação), inventário de certificados, alertas de validade e trilhas de auditoria, reduzindo falhas e retrabalho.
- **Eficiência administrativa**: eliminação de papel, automatização de fluxos, redução de deslocamentos para validação presencial (com AR por videoconferência quando cabível) e maior agilidade na formalização de atos.
- **Escalabilidade e capacidade de atendimento**: acomodação do crescimento previsto (~30%) de usuários e sistemas, com elasticidade de quantitativos e suporte compatível com a expansão da demanda.
- **Integração com ecossistema governamental**: compatibilidade com plataformas e sistemas federais, estaduais e municipais, incluindo representação institucional via e-CNPJ para matriz, filiais e fundos.
- **Previsibilidade orçamentária**: contratação estruturada por itens e perfis, com TCO mensurável e projeção plurianual de custos, favorecendo planejamento e execução do orçamento.
- **Melhoria da experiência do usuário**: prazos de emissão/renovação definidos, canais de suporte e orientação padronizados, reduzindo tempo de espera e incidentes operacionais.
- **Rastreabilidade e auditorabilidade**: registros consolidados de emissões, renovações, revogações e incidentes, facilitando controles internos, respostas a órgãos de controle e prestação de contas.
- **Alinhamento estratégico**: atendimento às metas do **PDTIC 2024–2027** (transformação digital, segurança cibernética, modernização e sustentabilidade), fortalecendo a governança de TIC do MJSP.
- **Sustentabilidade**: avanço do “papel zero” e redução de custos indiretos (armazenagem, logística e tempo de processamento), com impacto positivo em eficiência e meio ambiente.

17. Providências a serem Adotadas

17.1. Nos termos da alínea “e”, inciso II, do art. 11 da **IN SGD/ME nº 1/2019**, **não há providências a serem adotadas** pelo MJSP para viabilizar a execução contratual. A infraestrutura tecnológica, os perfis de acesso, as integrações com sistemas estruturantes (p.ex., SIAFI e SEI) e os procedimentos operacionais já se encontram implantados e aderentes aos requisitos da solução.

17.2. Eventuais ajustes operacionais de rotina (ex.: cadastramentos de novos usuários, emissões e renovações) serão absorvidos pelos **processos padrão de gestão do contrato**, não demandando adequações específicas de ambiente, aquisição de equipamentos ou mudanças organizacionais adicionais.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

18.1. O Estudo Técnico Preliminar desta contratação enfatiza que a abordagem mais eficaz para alcançar os resultados desejados, minimizar riscos e aderir aos princípios de economia, eficácia e eficiência é conduzir um processo de contratação do cenário 2 (contratação de serviços gerenciados de segurança da informação por valor fixo mensal), desde que sejam adotadas as premissas e conclusões descritas neste estudo, conforme preconizado na IN nº 94, de 23 de dezembro de 2022.

18.2. Dos benefícios esperados com a contratação:

18.2.1. Da Eficácia: A contratação permitirá o funcionamento adequado e contínuo dos sistemas e serviços de TIC essenciais à atividade institucional, garantindo alta disponibilidade e suporte técnico qualificado. Isso assegura que as soluções tecnológicas cumpram plenamente seu propósito, sem interrupções prejudiciais à missão do órgão. Os serviços permitirão ainda a proteção proativa contra ameaças cibernéticas, com atuação especializada em detecção, resposta e contenção de incidentes, promovendo a integridade, disponibilidade e autenticidade das informações, pilares essenciais para os serviços públicos digitais.

18.2.2. Da Eficiência: A contratação viabiliza a otimização dos recursos tecnológicos e humanos, reduzindo retrabalhos, indisponibilidades e intervenções corretivas emergenciais. Ao contratar serviços especializados adequados, será possível maximizar a produtividade da equipe interna de TIC e reduzir o tempo médio de resposta a incidentes.

18.2.3. Da Efetividade: Espera-se um impacto positivo direto nos resultados institucionais, pois a contratação dos serviços permite um avanço concreto e mensurável na maturidade da segurança da informação institucional, com a adoção de modelos reconhecidos internacionalmente e a implementação de controles de acordo com normas como ISO/IEC 27001, NIST e CIS. A integração desses serviços com ações de capacitação técnica assegura a transferência de conhecimento e a sustentabilidade das melhorias implantadas, resultando em impactos duradouros na política de segurança do órgão.

18.2.4. Da Economicidade: O cenário escolhido mostrou-se mais vantajoso após a análise de alternativas e os requisitos normativos, considerando o custo total de propriedade (TCO) e a prestação de serviços de segurança com pagamento fixo mensal vinculado ao cumprimento de Niveis Mínimos de Serviços (NMS) previamente estabelecidos. Ao prevenir falhas, minimizar interrupções, incidentes e reduzir gastos com manutenções corretivas, a contratação contribuirá para o uso racional e responsável dos recursos públicos. Além disso, a redução de impactos operacionais e reputacionais, a antecipação de vulnerabilidades e a conformidade com a LGPD e demais normativos da Administração Pública resultam em menor passivo jurídico e maior estabilidade institucional.

18.3. Dessa forma, a contratação de serviços gerenciados de segurança da informação apresenta-se como tecnicamente viável, estrategicamente alinhada e financeiramente justificável, cumprindo os critérios da IN nº 94/2022 e contribuindo significativamente para o fortalecimento da governança, da resiliência cibernética e da continuidade dos serviços públicos digitais.

18.4. Diante do exposto, a equipe de planejamento declara ser viável a contratação do cenário pretendido.

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.

Despacho: Portaria de Pessoal SAA/SE/MJSP Nº 58, de 8 de agosto de 2025

ALESSANDRA VOLPI GOULIN DE OLIVEIRA

Integrante Administrativo

Assinou eletronicamente em 26/02/2026 às 22:50:48.

Despacho: Portaria de Pessoal SAA/SE/MJSP Nº 58, de 8 de agosto de 2025

ARTUR HENRIQUE CASTRO DE ANDRADE

Integrante Requisitante

Assinou eletronicamente em 26/02/2026 às 18:36:13.

Despacho: Portaria de Pessoal SAA/SE/MJSP Nº 58, de 8 de agosto de 2025

FABIANO DA CRUZ

Integrante Técnico

Assinou eletronicamente em 25/02/2026 às 11:32:18.

SOLANGE BERTO DE MEDEIROS

Autoridade competente

Assinou eletronicamente em 27/02/2026 às 11:28:16.