ESP-DEPTO.SUPR.ATIVIDADES COMPLEMENTARES

Estudo Técnico Preliminar 9/2026

1. Informações Básicas

Número do processo: 023.00000470/2026-61

2. Descrição da necessidade

2.1. A PGE necessita manter e ampliar meios de identificação digital, autenticação e assinatura digital com validade jurídica em ambientes eletrônicos, bem como assegurar proteção criptográfica confiável de serviços web institucionais. A ausência, insuficiência ou expiração de certificados impacta diretamente a continuidade das atividades, a integridade de transações eletrônicas e a confiabilidade de acessos a serviços digitais.

3. Área requisitante

Área Requisitante	Responsável
Coordenadoria de Suprimentos e Atividades Complementares - CSAC	Mariana Sancia de Souza

4. Necessidades de Negócio

4.1. 4.1. A contratação visa assegurar continuidade operacional e conformidade na prática de atos digitais (assinatura, autenticação e comunicação eletrônica), além de reforçar a segurança e a confiança dos serviços web institucionais mediante SSL OV com validação organizacional, reduzindo riscos de indisponibilidade, falhas de autenticação e exposição a vulnerabilidades.
4.2. Adicionalmente, a necessidade de negócio compreende a garantia de suporte técnico de alta disponibilidade e eficiência, estabelecendo parâmetros mínimos de desempenho (SLA) para mitigar o risco de paralisação de processos administrativos e judiciais .A solução deve assegurar tempos de resposta e solução céleres (estimados em 2h para resposta e 8h para solução), evitando que falhas técnicas na emissão ou uso dos certificados comprometam a tempestividade das atividades da Procuradoria.
4.3. Busca-se, ainda, a integração logística e operacional que minimize o tempo entre a solicitação e a efetiva entrega dos certificados e mídias, atendendo à demanda por mobilidade e segurança dos usuários críticos, conforme os prazos máximos de emissão previstos para evitar interrupções operacionais.

5. Necessidades Tecnológicas

5.1. A solução tecnológica deverá contemplar, obrigatoriamente:
5.1.1. Conformidade Normativa: Certificados e-CPF e e-CNPJ emitidos em total observância aos padrões da ICP-Brasil, garantindo integridade, autenticidade e validade jurídica.
5.1.2. Flexibilidade de Mídias: Atendimento às modalidades A1 (arquivo digital para computador/dispositivos móveis) e A3 (armazenados em token ou cartão inteligente com leitora), incluindo a possibilidade de emissão "somente certificado" para usuários que já possuam mídia homologada.
5.1.3. Compatibilidade de Ambiente: A solução deve ser plenamente funcional em ambiente Microsoft Windows 10, sistema para o qual a contratada disponibilizará guias e drivers de instalação.
5.1.4. Limitações de Escopo Técnico: Em alinhamento com a viabilidade técnica da solução, ficam excluídos do escopo de compatibilidade os sistemas operacionais Windows Server, Macintosh, Linux, bem como versões obsoletas do Windows (XP, 7 e Vista), devendo a TI da PGE validar previamente a aderência do parque tecnológico a estas restrições.
5.1.5. Segurança Web (SSL OV): Fornecimento de Certificado SSL Standard – OV (Raiz Internacional) com criptografia de comunicações (HTTPS) e validação organizacional, assegurando a aceitabilidade nos principais navegadores (Chrome, Safari, Edge) e conformidade com os princípios de

segurança da LGPD.
5.1.6. Rastreabilidade: Procedimentos de validação (presencial ou por videoconferência) com coleta biométrica e foto da face, além de mecanismos de revogação de certificados durante a vigência

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

6.1. Além dos requisitos técnicos, deverão ser previstos como critérios de aceitação e execução:

6.1.1. Fluxo Operacional e Logística de Vouchers: O fluxo de solicitações deve ser rastreável, garantindo que os vouchers para emissão sejam enviados à PGE em até 07 (sete) dias úteis após a solicitação. O gerenciamento dos vouchers e o agendamento da identificação (presencial ou por videoconferência) serão responsabilidade da contratante, mediante site disponibilizado pela contratada.
6.1.2. Suporte Técnico e Níveis de Serviço (SLA): Como medida preventiva ao risco de paralisação de processos (Risco R-03), o suporte técnico deverá estar disponível de segunda a sexta-feira, das 8h às 19h. Os níveis críticos de atendimento devem observar o tempo máximo de 02 (duas) horas para resposta e 08 (oito) horas para a solução definitiva de incidentes que impeçam a emissão ou uso dos certificados.
6.1.3. Prazos de Emissão e Prazos Fatais Regulatória: A contratada deve assegurar capacidade operacional para emissão imediata após a validação presencial/videoconferência. Especificamente para os itens e-CNPJ A3 (36 meses), a solução deve garantir a emissão até o prazo limite de março de 2026, conforme a Resolução nº 211/2024 da ICP-Brasil, sob pena de inexecução contratual.
6.1.4. Regras de Segurança e Validação: O processo de emissão deve obrigatoriamente incluir a coleta de biometria das impressões digitais e foto da face, conforme normas da ICP-Brasil, realizada por Agente de Registro credenciado.
6.1.5. Critérios de Aceitação do SSL OV: A aceitabilidade do certificado SSL Standard - OV está condicionada ao reconhecimento por cadeias de confiança de fabricantes como Google (Chrome), Apple (Safari) e Microsoft (Edge). A contratada deve comprovar a realização da validação jurídica da organização e da posse do domínio em um prazo de 07 a 12 dias corridos.
6.1.6. Gestão e Fiscalização: Devem ser fornecidos relatórios mensais de emissões (por item, unidade e status), permitindo a conferência e a atestação da nota fiscal em até 03 dias pela Administração. A contratada deve disponibilizar serviço de revogação de certificados durante todo o período de vigência.
6.1.7. Restrições de Compatibilidade: A solução deve prever suporte e drivers específicos para Windows 10, ficando estabelecido que a incompatibilidade com sistemas Macintosh, Linux ou versões obsoletas do Windows (XP, 7 e Vista) não será motivo para sanções à contratada, desde que previamente informado

6.1.1. Fluxo Operacional e Logística de Vouchers: O fluxo de solicitações deve ser rastreável, garantindo que os vouchers para emissão sejam enviados à PGE em até 07 (sete) dias úteis após a solicitação. O gerenciamento dos vouchers e o agendamento da identificação (presencial ou por videoconferência) serão responsabilidade da contratante, mediante site disponibilizado pela contratada.
6.1.2. Suporte Técnico e Níveis de Serviço (SLA): Como medida preventiva ao risco de paralisação de processos (Risco R-03), o suporte técnico deverá estar disponível de segunda a sexta-feira, das 8h às 19h. Os níveis críticos de atendimento devem observar o tempo máximo de 02 (duas) horas para resposta e 08 (oito) horas para a solução definitiva de incidentes que impeçam a emissão ou uso dos certificados.
6.1.3. Prazos de Emissão e Prazos Fatais Regulatória: A contratada deve assegurar capacidade operacional para emissão imediata após a validação presencial/videoconferência. Especificamente para os itens e-CNPJ A3 (36 meses), a solução deve garantir a emissão até o prazo limite de março de 2026, conforme a Resolução nº 211/2024 da ICP-Brasil, sob pena de inexecução contratual.
6.1.4. Regras de Segurança e Validação: O processo de emissão deve obrigatoriamente incluir a coleta de biometria das impressões digitais e foto da face, conforme normas da ICP-Brasil, realizada por Agente de Registro credenciado.
6.1.5. Critérios de Aceitação do SSL OV: A aceitabilidade do certificado SSL Standard - OV está condicionada ao reconhecimento por cadeias de confiança de fabricantes como Google (Chrome), Apple (Safari) e Microsoft (Edge). A contratada deve comprovar a realização da validação jurídica da organização e da posse do domínio em um prazo de 07 a 12 dias corridos.
6.1.6. Gestão e Fiscalização: Devem ser fornecidos relatórios mensais de emissões (por item, unidade e status), permitindo a conferência e a atestação da nota fiscal em até 03 dias pela Administração. A contratada deve disponibilizar serviço de revogação de certificados durante todo o período de vigência.

6.1.7. Restrições de Compatibilidade: A solução deve prever suporte e drivers específicos para Windows 10, ficando estabelecido que a incompatibilidade com sistemas Macintosh, Linux ou versões obsoletas do Windows (XP, 7 e Vista) não será motivo para sanções à contratada, desde que previamente informado

"Quadro Resumo de Requisitos para o Termo de Referência"

Tema	Requisito mínimo (descrição para o Termo de Referência)
Emissão / Validação	Processo rastreável com envio de vouchers em até **07 (sete) dias úteis** após solicitação. Validação obrigatoriamente vinculada à coleta de **biometria das impressões digitais e foto da face**, conforme normas da ICP-Brasil.
Suporte Técnico	Central de atendimento disponível de segunda a sexta, das **8h às 19h**. Nível de serviço (**SLA**) de resposta em até **02 (duas) horas** e solução definitiva em até **08 (oito) horas** para evitar paralisação de processos judiciais.
Segurança e TI	Compatibilidade plena com o sistema operacional **Microsoft Windows 10**, com fornecimento de guias e drivers. Exclusão explícita de suporte para Windows Server, Macintosh, Linux e versões obsoletas (XP, 7 e Vista).
SSL OV	Certificado com validação da organização e do domínio, com prazo de conclusão do processo entre **07 a 12 dias corridos**. Garantia de aceitabilidade nos navegadores **Chrome, Safari e Edge**.
Gestão e Controle	Faturamento mensal por unidades efetivamente emitidas. Fornecimento de **relatórios mensais** contendo item, unidade requisitante e status, além de serviço de revogação disponível durante a vigência

7. Estimativa da demanda - quantidade de bens e serviços

7.1. A estimativa dos quantitativos apresentados neste Estudo Técnico Preliminar foi elaborada com base na análise do histórico de utilização de certificados digitais no âmbito da Procuradoria Geral do Estado, bem como na projeção de necessidades decorrentes da continuidade e ampliação do uso de processos eletrônicos, sistemas institucionais e serviços digitais que exigem autenticação e assinatura eletrônica com validade jurídica.

7.1.1. Foram considerados, para a definição dos quantitativos:

- o número estimado de procuradores, servidores e unidades administrativas que necessitam de certificados digitais para o desempenho regular de suas atividades;
- o histórico de emissões e renovações de certificados digitais realizadas em contratações anteriores;
- a necessidade de substituição periódica dos certificados conforme seus prazos de validade (12 ou 36 meses);
- a previsão de novas emissões decorrentes de ingresso de servidores, substituições de titulares e atualização tecnológica dos sistemas institucionais;
- a necessidade de manutenção de certificados SSL válidos para proteção criptográfica de serviços web institucionais.

7.1.2. Assim, os quantitativos estimados refletem demanda institucional projetada para o período contratual, considerando a necessidade de garantir a continuidade das atividades administrativas e jurídicas que dependem de autenticação digital segura, bem como a proteção dos serviços web da instituição.

7.2. Tabela de Quantitativos

DENOMINAÇÃO DOS SERVIÇOS		CADSER	UNIDADE DE MEDIDA	Q T D E . ESTIMADA
5.1	**CERTIFICADO DIGITAL PARA PESSOA FÍSICA E JURÍDICA**			
5.1.1	**Certificado Digital para Pessoa Física e-CPF**			
5.1.1.1	**Certificado e-CPF A3 em token – 36 meses Gov**	27189	**Unidade**	**200**
5.1.1.2	**Certificado e-CPF A3 (somente certificado) – 36 meses Gov**	27219	**Unidade**	**200**
5.1.1.3	**e-CPF A1 – 12 meses (Gov)**	27146	**Unidade**	**300**
5.1.2	**Certificado Digital para Pessoa Jurídica e-CNPJ**			
5.1.2.1	**e-CNPJ A1 – 12 meses (Gov)**	27162	**Unidade**	**30**
5.1.2.2	**Certificado e-CNPJ A3 em token – 36 meses Gov**	27197	**Unidade**	**25**
5.1.2.3	**Certificado e-CNPJ A3 em token – 12 meses Gov**	27197	**Unidade**	**25**
5.1.3	**Diária de Validação Externa**			
5.1.3.1	**Diária de Validação Externa**	27162	**Unidade**	**25**
5.2	**CERTIFICADO DIGITAL SSL RAIZ INTERNACIONAL**			
5.2.1	**Cerificado digital tipo SSL Standard – OV – 12 meses**	30274	**Unidade**	**10**

8. Levantamento de soluções

8. Este item registra as alternativas avaliadas para atendimento da necessidade e suas implicações. Foram consideradas :
8.1.1. contratação integrada para emissão de certificados ICP Brasil (e CPF/e CNPJ) nas modalidades A1/A3, com suporte e possibilidade de validação externa;
8.1.2. contratação de SSL OV com raiz internacional para serviços web institucionais;
8.1.3. alternativa de separar contratações (um fornecedor para ICP Brasil e outro para SSL), considerada possível, porém com maior custo indireto de gestão e fiscalização (mais instrumentos e interfaces operacionais).

9. Análise comparativa de soluções

9.1. Comparação entre as soluções possíveis para atendimento da necessidade, sob os aspectos técnico, operacional e econômico, justificando a escolha da solução mais vantajosa para a Administração.

9.1.1. Tabela – Análise comparativa das soluções avaliadas

Solução analisada	Descrição resumida	Vantagens	Desvantagens / Riscos	Avaliação
Solução 1 – Contratação integrada (ICPBrasil + SSL OV) (Escolhida)	Contratação de empresa para emissão de eCPF e eCNPJ (A1/A3), com diária de validação externa, e fornecimento de SSL Standard OV (raiz internacional), conforme quantitativos estimados.	• Atendimento integral da necessidade • Validade jurídica garantida (ICPBrasil) • SSL OV com ampla aceitação em navegadores • Menor custo indireto de gestão • Medição objetiva por unidade/diária • Maior previsibilidade operacional	• Dependência de um único fornecedor • Necessidade de fiscalização técnica adequada	**Mais vantajosa** do ponto de vista técnico, operacional e econômico
Solução 2 – Contratações separadas (ICPBrasil + SSL em contratos distintos)	Um contrato para eCPF/eCNPJ e outro contrato para SSL OV raiz internacional.	• Especialização por tipo de serviço • Redução de dependência de fornecedor único	• Maior custo administrativo • Duplicidade de gestão e fiscalização • Maior risco de desalinhamento de prazos (expiração de SSL x certificados pessoais) • Aumento de custos indiretos	**Menos eficiente** sob o aspecto da economicidade global
Solução 3 – Uso exclusivo de certificados A1 (sem A3)	Emissão apenas de certificados A1 para PF e PJ, sem uso de A3.	• Menor custo unitário • Facilidade de instalação	• Menor nível de segurança • Inadequado para perfis sensíveis • Maior risco operacional e jurídico	**Inadequada** para o perfil institucional

Solução 4 – Uso de SSL autoassinado ou sem raiz internacional	Proteção de serviços web com certificados sem cadeia pública confiável.	• Baixo custo inicial	• Alertas de segurança em navegadores • Quebra de confiança do usuário • Risco institucional e reputacional	**Inviável tecnicamente**
Solução 5 – Não contratação (manutenção do cenário atual)	Manutenção sem renovação/emissão sistemática de certificados.	• Nenhum desembolso imediato	• Risco de expiração de certificados • Paralisação de atividades • Invalidade de atos digitais	**Inviável**

9.1.2. Síntese da análise comparativa

A Solução 1 – Contratação integrada mostra-se a mais vantajosa, pois:

- atende integralmente às necessidades de assinatura, autenticação e segurança web;
- assegura conformidade jurídica (ICP Brasil) e confiabilidade técnica (SSL OV raiz internacional);
- reduz custos indiretos de gestão, fiscalização e coordenação;
- permite flexibilidade operacional, ao contemplar A1, A3 com token e A3 “somente certificado”;
- viabiliza planejamento financeiro, com quantitativos definidos e medição objetiva.

As demais soluções apresentam desvantagens relevantes, seja por aumento de custos administrativos, seja por risco técnico, jurídico ou operacional, não se mostrando adequadas ao interesse público.

10. Registro de soluções consideradas inviáveis

10.1. Descarte de alternativas que não atendem aos requisitos essenciais ou ampliam riscos indevidos. Foram consideradas inviáveis:

10.1.1. soluções de certificação para assinatura/autenticação que não observem o arcabouço ICP Brasil quando exigida validade jurídica;

10.1.2. uso de SSL autoassinado ou de cadeia não reconhecida publicamente para serviços expostos;

10.1.3. emissão/gestão sem fluxo mínimo de rastreabilidade e suporte, por elevar risco de falhas, indisponibilidade e retrabalho.

11. Análise comparativa de custos (TCO)

11.1. A análise de TCO considera os custos diretos por emissão e validade (12m/36m), custos de mídia (quando aplicável), diárias de validação externa, gestão operacional (agendamento, controle de validade, revogação e suporte) e custos indiretos associados a indisponibilidade e retrabalho.

Annualização (TCO) para itens com validade de 36 meses (comparação anual)

Observação: para comparar custos anuais entre certificados de 12 e 36 meses, aplica-se annualização simples (divisão por 3) aos itens de 36 meses.

Item (36 meses)	Qtde	Total (R$)	Total anualizado (R$)
eCPF A3 com token – 36m	200	55.420,00	18.473,33

eCPF A3 somente cert. – 36m	200	33.452,00	11.150,67
eCNPJ A3 com token – 36m	25	7.128,75	2.376,25

Nota de gestão: a annualização serve para análise comparativa (TCO). O desembolso contratual seguirá o modelo de medição/pagamento pactuado.

12. Descrição da solução de TIC a ser contratada

12.1. A solução de TIC a ser contratada consiste na prestação de serviços especializados de certificação digital, compreendendo a emissão, renovação, suporte e validação de certificados digitais e CPF e e CNPJ, em conformidade com as normas e procedimentos da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil, bem como o fornecimento de Certificados Digitais SSL Standard – OV (Organization Validation), com raiz internacional, destinados à proteção de serviços web institucionais.
A solução contempla, de forma integrada e sob demanda, os seguintes componentes:
a) Certificados Digitais para Pessoa Física (e CPF):
Emissão de certificados nas modalidades:
- A1, com validade de 12 meses;
- A3, com validade de 36 meses, com fornecimento de mídia criptográfica (token);
- A3 “somente certificado”, com validade de 36 meses, para titulares que já possuam mídia criptográfica compatível.

b) Certificados Digitais para Pessoa Jurídica (e CNPJ):
Emissão de certificados nas modalidades:
- A1, com validade de 12 meses;
- A3, com validade de 12 e 36 meses, com fornecimento de mídia criptográfica (token), conforme quantitativos estimados e perfil de uso institucional.

c) Serviço de Diária de Validação Externa:
Prestação de serviço de validação presencial in loco, por Agente de Registro credenciado, destinado a viabilizar o atendimento concentrado de titulares em unidades da PGE, quando necessário, otimizando o fluxo de emissões, reduzindo deslocamentos e mitigando riscos de atraso ou indisponibilidade operacional.
d) Certificado Digital SSL Standard – OV (Raiz Internacional):
Fornecimento de certificados SSL/TLS do tipo Organization Validation, com validade de 12 meses, emitidos por Autoridade Certificadora de raiz internacional amplamente reconhecida, garantindo:
- criptografia de comunicações web (HTTPS);
- validação da identidade organizacional da PGE;
- compatibilidade com navegadores e sistemas operacionais amplamente utilizados;
- mitigação de alertas de segurança e riscos reputacionais.

A execução da solução deverá observar processo estruturado e rastreável, contemplando solicitação, validação, emissão, entrega, suporte técnico, reemissão e revogação de certificados, com medição mensal por unidades efetivamente emitidas e serviços efetivamente prestados, permitindo adequada fiscalização, ateste e controle contratual.
A solução descrita foi selecionada por demonstrar aderência integral às necessidades institucionais, compatibilidade técnica, segurança jurídica, eficiência operacional e economicidade, conforme evidenciado na análise comparativa de soluções e na estimativa de custos constantes deste Estudo Técnico Preliminar.

13. Estimativa de custo total da contratação

Valor (R$): 165.838,50

13.1. O custo total da contratação está descrita na tabela abaixo:

DENOMINAÇÃO DOS SERVIÇOS		UNIDADE D E MEDIDA	QTDE. ESTIMADA	VALOR UNITÁRIO	TOTAL
5.1	CERTIFICADO DIGITALPARA PESSOA FÍSICA E JURÍDICA				R$ 156.689,20
5.1.1	Certificado Digital para Pessoa Física e-CPF				R$ 126.369,00
5.1.1.1	Certificado e-CPF A3 em token - 36 meses Gov	UNIDADE	200	R$ 277,10	R$ 55.420,00
	Certificado e-CPF A3 (somente certificado) - 36 meses				

5.1.1.2	Gov	UNIDADE	200	R$ 167,26	R$ 33.452,00
5.1.1.3	e-CPF A1 - 12 meses (Gov)	UNIDADE	300	R$ 124,99	R$ 37.497,00
5.1.2	Certificado Digital para Pessoa Jurídica e-CNPJ				R$ 16.258,70
5.1.2.1	e-CNPJ A1 - 12 meses (Gov)	UNIDADE	30	R$ 139,39	R$ 4.181,70
5.1.2.2	Certificado e-CNPJ A3 em token - 36 meses Gov	UNIDADE	25	R$ 285,15	R$ 7.128,75
5.1.2.3	Certificado e-CNPJ A3 em token - 12 meses Gov	UNIDADE	25	R$ 197,93	R$ 4.948,25
5.1.3	Diária de Validação Externa				R$ 14.061,50
5.1.3.1	Diária de Validação Externa	UNIDADE	25	R$ 562,46	R$ 14.061,50
5.2	CERTIFICADO DIGITAL SSL RAIZ INTERNACIONAL				R$ 9.149,30
5.2.1	Certificado digital tipo SSL Standard - OV - 12 meses	UNIDADE	10	R$ 914,93	R$ 9.149,30
TOTAL (12 MESES)					R$ 165.838,50

13.2. Consideradas as alternativas avaliadas neste Estudo Técnico Preliminar, verifica-se o enquadramento jurídico da demanda na hipótese de dispensa de licitação prevista no art. 75, inciso IX, da Lei nº 14.133/2021, que autoriza a contratação direta de serviços prestados por órgão ou entidade integrante da Administração Pública, instituídos e estruturados para esse fim específico, desde que o preço seja compatível com o praticado no mercado.

13.3. Nesse contexto, identifica-se como solução apta ao atendimento da demanda a contratação da PRODESP – Companhia de Processamento de Dados do Estado de São Paulo, entidade integrante da Administração Pública estadual, para a prestação dos serviços de certificação digital descritos neste ETP, por se tratar de atividade compatível com suas finalidades institucionais.

13.4. A formalização da contratação com fundamento no art. 75, inciso IX, ficará condicionada à comprovação, nos autos, de forma cumulativa, dos seguintes requisitos legais:

- aderência do objeto às finalidades institucionais da PRODESP;
- comprovação de que os serviços de certificação digital encontram-se institucionalmente criados, estruturados e mantidos para essa finalidade específica; e
- demonstração da vantajosidade econômica da contratação, mediante pesquisa comparativa de preços e/ou documentação idônea que comprove a compatibilidade dos valores propostos com os praticados no mercado.

13.5. Ressalta-se que o Estudo Técnico Preliminar tem por finalidade identificar a necessidade administrativa, a solução adequada e o respectivo enquadramento jurídico, não se destinando à formalização da escolha definitiva da entidade prestadora. A confirmação do enquadramento legal, a motivação específica da escolha e a juntada das evidências comprobatórias ocorrerão na fase de instrução da contratação, por meio do Termo de Referência, da justificativa técnica e do ato formal de dispensa.

13.6. Na hipótese de não restar comprovado o atendimento integral dos requisitos previstos no art. 75, inciso IX, da Lei nº 14.133/2021, a Administração deverá adotar procedimento de contratação diverso, devidamente motivado, dentre aqueles previstos na legislação vigente.

14. Justificativa técnica da escolha da solução

14.1. A solução selecionada apresenta plena adequação técnica ao atender, de forma integrada e padronizada, às necessidades de identificação digital, autenticação, assinatura eletrônica com validade jurídica e proteção de serviços web institucionais, reduzindo riscos operacionais e assegurando a continuidade dos serviços digitais da PGE.

14.1.1. Aderência normativa e validade jurídica

A emissão de certificados e CPF e e CNPJ em conformidade com os padrões da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil garante a validade jurídica, a autenticidade, a integridade e o não repúdio nas assinaturas e transações eletrônicas, requisito técnico indispensável para a atuação institucional. Soluções que não observem esse ecossistema não atendem aos requisitos legais e técnicos exigidos.

14.1.2. Compatibilidade técnica com diferentes perfis de uso

A solução contempla as modalidades A1 e A3, permitindo adequação ao perfil de risco, mobilidade e criticidade dos usuários:

- o A1 atende demandas de uso corrente e temporário, com simplicidade operacional;
- o A3, em mídia criptográfica, oferece maior nível de segurança para perfis sensíveis ou de uso institucional contínuo;
- a previsão de A3 “somente certificado” assegura flexibilidade técnica, evitando duplicidade de mídias quando o titular já dispõe de token compatível, sem comprometer segurança ou conformidade.

14.1.3. Robustez operacional e escalabilidade

A inclusão do serviço de Diária de Validação Externa confere robustez operacional à solução, permitindo:

- atendimento concentrado de múltiplos titulares;
- redução de gargalos de agendamento;
- mitigação de riscos de atraso na emissão e renovação de certificados;
- maior previsibilidade operacional em demandas pontuais ou sazonais. Essa característica técnica aumenta a resiliência do serviço e reduz impactos sobre as unidades administrativas.

14.1.4. Segurança e confiabilidade de serviços web

A adoção de Certificados SSL Standard – OV (Raiz Internacional) atende aos requisitos técnicos para proteção de ambientes web institucionais, assegurando:

- criptografia das comunicações;
- validação da identidade organizacional da PGE;
- compatibilidade com os principais navegadores e sistemas operacionais;
- redução de alertas de segurança e riscos de indisponibilidade por rejeição de cadeia de confiança. Do ponto de vista técnico, esta solução é a mais adequada para serviços expostos à internet, garantindo confiabilidade e aceitação ampla.

14.1.5. Padronização, suporte e governança técnica

A solução selecionada pressupõe processo estruturado e rastreável de emissão, renovação, suporte, reemissão e revogação, permitindo:

- padronização técnica dos certificados utilizados;
- melhor controle de ciclo de vida, validade e inventário;
- facilitação da fiscalização e do ateste técnico;
- redução de falhas humanas e retrabalho. Esses aspectos são fundamentais para a governança de TIC e a segurança da informação institucional.

14.1.6. Conclusão técnica

Diante do exposto, resta comprovado que a solução escolhida:

- é tecnicamente necessária e suficiente para atendimento da demanda;
- atende aos requisitos normativos, funcionais e de segurança;
- apresenta flexibilidade, escalabilidade e robustez operacional;
- e se mostra compatível com a infraestrutura, os processos e o perfil de uso da PGE.

Assim, a escolha da solução revela se tecnicamente adequada e justificada, atendendo aos princípios da eficiência, da segurança da informação e da continuidade do serviço público.

15. Justificativa econômica da escolha da solução

15.1. A solução selecionada (emissão de e-CPF e e-CNPJ conforme ICP-Brasil, com Diária de Validação Externa quando necessária, e fornecimento de SSL Standard – OV (Raiz Internacional)) apresenta-se economicamente mais vantajosa por atender integralmente às necessidades institucionais com custos estimados definidos, mecanismo de medição por unidade/serviço efetivamente prestado e redução de custos indiretos associados à gestão do ciclo de vida dos certificados.

15.1 – Adequação do custo ao objeto (custo direto mensurável)

O valor estimado total para 12 meses é de R$ 165.838,50, composto por certificados ICP-Brasil (PF/PJ), diárias de validação externa e SSL OV. A estrutura de itens e quantitativos permite planejamento orçamentário e controle de execução por medição objetiva (unidades emitidas e diárias executadas), reduzindo o risco de pagamentos por serviços não utilizados.

Componente da contratação	**Descrição**
Certificados ICPBrasil – Pessoa Física	Emissão de eCPF nas modalidades A1 e A3 (com e sem token)
Certificados ICPBrasil – Pessoa Jurídica	Emissão de eCNPJ nas modalidades A1 e A3 (12 e 36 meses)
Diária de Validação Externa	Atendimento presencial in loco por Agente de Registro, quando necessário
Certificado SSL Standard – OV	Certificados SSL/TLS com validação organizacional e raiz internacional
Valor estimado total (12 meses)	**R$ 165.838,50**

15.2 – Economicidade pelo ciclo de vida (validades de 12 e 36 meses)

A solução contempla certificados com validade de 12 meses e de 36 meses, o que favorece a economicidade em perfis de uso contínuo, pois reduz recorrência de renovações, retrabalho administrativo e risco de interrupções por expiração. Para efeito comparativo (TCO), os certificados de 36 meses podem ser annualizados (divisão por 3), permitindo evidenciar custo anual equivalente e apoiar a decisão de adoção por perfil.

Annualização (comparação anual) dos itens de 36 meses

Item (validade de 36 meses)	**Valor total (R$)**	**Custo anual equivalente (R$)**
eCPF A3 com token	55.420,00	18.473,33
eCPF A3 – somente certificado	33.452,00	11.150,67
eCNPJ A3 com token	7.128,75	2.376,25

Nota: a annualização consiste na divisão do valor total pela validade (36 meses), sendo utilizada exclusivamente para fins de **análise comparativa de custo total de propriedade (TCO)**, não alterando a forma de medição ou pagamento prevista no contrato.

15.3 – Redução de custos indiretos (operação e governança)

A contratação integrada reduz custos indiretos e riscos operacionais ao:

a) permitir emissão padronizada e rastreável (reduz tempo de atendimento interno e retrabalho);

b) ofertar A3 “somente certificado” para titulares que já possuem token compatível, evitando gasto desnecessário com mídias quando não requerido;

c) prever Diária de Validação Externa, que concentra atendimentos e reduz deslocamentos, ausências e tempos improdutivos — mitigando atrasos e impactos na continuidade de atividades;

d) incluir SSL OV raiz internacional, reduzindo riscos de alertas/bloqueios de navegação e indisponibilidade de serviços web por certificados inadequados, com consequente prevenção de custos reativos (correções emergenciais, substituições intempestivas e impacto reputacional).

Medida adotada na solução	**Impacto econômico**
Emissão padronizada e rastreável	Redução de tempo administrativo e retrabalho
A3 “somente certificado”	Evita aquisição desnecessária de tokens
Diária de Validação Externa	Reduz deslocamentos, ausências e tempo improdutivo
SSL OV com raiz internacional	Previne indisponibilidades, alertas e correções emergenciais
Contratação integrada (ICPBrasil + SSL)	Diminui custo de gestão e fiscalização contratual

15.4 – Custo evitado e mitigação de riscos (economicidade ampliada)

A escolha também é economicamente justificada pelo custo evitado decorrente da mitigação de riscos típicos:

• interrupção de operações por expiração de certificados e paralisação de atividades digitais;

• retrabalho e reemissões por falhas de validação/instalação sem suporte adequado;

• perda de confiabilidade e indisponibilidade de serviços web por ausência/insuficiência de SSL adequado;

• aumento de custo administrativo com múltiplos contratos e múltiplas fiscalizações (separação ICP-Brasil vs SSL), o que elevaria o custo indireto de gestão

Risco mitigado	**Custo evitado**
Expiração de certificados	Paralisação de atividades digitais
Falhas de validação/instalação	Reemissões, retrabalho e suporte corretivo
SSL inadequado ou inexistente	Indisponibilidade de serviços web e impacto reputacional
Múltiplas contratações	Aumento de custo administrativo e de fiscalização

15.5 – Diante do exposto, a solução escolhida apresenta vantajosidade econômica por combinar:

16.5.1. atendimento integral da necessidade;

16.5.2. previsibilidade e controle do gasto por itens e quantitativos;

16.5.3. racionalidade no ciclo de vida (12/36 meses) com redução de custos recorrentes; e

16.5.4. redução de custos indiretos e de riscos operacionais. Assim, resta demonstrada a economicidade e adequação custo-benefício da solução selecionada para a PGE.

16. Alinhamento: Contratação e Planejamento

16.1. O objeto da contratação está previsto no Plano de Contratações Anual de 2025, nos termos do Decreto estadual nº 67.689, de 3 de maio de 2023, conforme detalhamento a seguir:
I) ID PCA no PNCP: ;71584833000195-0-000008/2026
II) Data de publicação no PNCP: ;23/05/2025
III) Id do item no PCA:330;
IV) Classe/Grupo: 167;
V) Identificador da Futura Contratação: 400102-128/2026.

17. Justificativa para o Parcelamento

17.1. Trata-se de contratação única, não sendo possível o parcelamento da contratação

18. Contratações Correlatas

18.1. Não se faz necessária a realização de contratações correlatas e/ou interdependentes para que o objetivo desta contratação seja atingido.

19. Benefícios a serem alcançados com a contratação

19.1. A contratação dos serviços de emissão de Certificados Digitais e CPF e e CNPJ (ICP Brasil), da Diária de Validação Externa e do Certificado SSL Standard – OV (Raiz Internacional) proporcionará à Procuradoria Geral do Estado benefícios relevantes e mensuráveis, distribuídos nos seguintes eixos:
19.1.1 – Benefícios institucionais e jurídicos
- Validade jurídica plena dos atos praticados em meio eletrônico, com garantia de autenticidade, integridade e não repúdio, em conformidade com o ecossistema ICP Brasil;
- Padronização institucional do uso de certificados digitais, reduzindo riscos de soluções improvisadas ou desconformes;
- Segurança jurídica nas interações com outros órgãos, sistemas governamentais, Poder Judiciário e terceiros;
- Mitigação de riscos de nulidade ou questionamentos sobre assinaturas e autenticações eletrônicas.

19.1.2 – Benefícios operacionais e de continuidade do serviço
- Continuidade das atividades administrativas e processuais, evitando interrupções decorrentes de expiração ou indisponibilidade de certificados;
- Redução de gargalos operacionais, por meio do atendimento concentrado e planejado, especialmente com a previsão da Diária de Validação Externa;
- Previsibilidade operacional, com planejamento de emissões e renovações ao longo da vigência contratual;
- Diminuição de retrabalho, decorrente de processos estruturados de emissão, suporte e revogação.

19.1.3 – Benefícios de segurança da informação
- Elevação do nível de segurança na autenticação e assinatura digital, com adequação ao perfil de risco dos usuários (A1 e A3);
- Proteção criptográfica dos serviços web institucionais, com uso de SSL OV de raiz internacional, amplamente aceito por navegadores e sistemas;
- Redução de incidentes de segurança relacionados a certificados inválidos, autoassinados ou cadeias de confiança não reconhecidas;
- Reforço da governança de identidades digitais, contribuindo para práticas mais maduras de segurança da informação.

19.1.4 – Benefícios econômicos e de eficiência administrativa
- Racionalização de custos, com utilização combinada de certificados de 12 e 36 meses, conforme perfil de uso e criticidade;
- Redução de custos indiretos, como tempo da equipe, deslocamentos desnecessários e correções emergenciais;
- Melhor controle do gasto público, com medição por unidades efetivamente emitidas e serviços efetivamente prestados;
- Aproveitamento de mídias existentes, por meio da emissão de certificados A3 “somente certificado”, quando aplicável.

19.1.5 – Benefícios reputacionais e de confiança institucional
- Aumento da confiança dos usuários internos e externos nos serviços digitais prestados pela PGE;
- Redução de alertas e bloqueios em ambientes web, preservando a imagem institucional em canais digitais;
- Demonstração de compromisso com boas práticas, segurança da informação e conformidade regulatória.

Em síntese, a contratação contribuirá de forma direta para a modernização segura, a continuidade operacional, a eficiência administrativa e a conformidade jurídica das atividades da Procuradoria Geral do Estado, agregando valor público e fortalecendo a governança de TIC e de segurança da informação.

20. Providências a serem Adotadas

20.1. Para a adequada implementação da solução de TIC descrita neste Estudo Técnico Preliminar, deverão ser adotadas providências prévias, concomitantes e posteriores à contratação, com vistas a garantir conformidade normativa, eficiência operacional, segurança da informação e efetiva fiscalização contratual.
Inicialmente, fazse necessária a consolidação definitiva da demanda, com a identificação dos titulares, unidades requisitantes e perfis de uso, bem como a definição de critérios objetivos para a escolha entre certificados A1 e A3, inclusive nos casos de emissão A3 “somente certificado”, de modo a compatibilizar nível de segurança, criticidade do uso e racionalidade de custos.
20.2. Deverá ser elaborado Termo de Referência alinhado integralmente ao presente ETP, contemplando de forma clara e suficiente: os requisitos técnicos e operacionais; os fluxos de solicitação, validação, emissão, reemissão e revogação de certificados; os níveis mínimos de serviço (SLA); os critérios de medição, ateste e pagamento; as responsabilidades da contratada e da contratante; bem como as hipóteses de penalidades por descumprimento contratual.
20.3. No âmbito da execução, será necessário estruturar a governança do contrato, com a designação formal de gestor e fiscais, definição de rotinas de acompanhamento, controle de validade dos certificados, registro de ocorrências, controle de revogações e reemissões, além da verificação periódica da aderência do serviço prestado aos requisitos estabelecidos.
20.4. Deverão ser organizadas, quando demandadas, as atividades de validação externa (in loco), incluindo planejamento de agenda, infraestrutura

mínima para atendimento, comunicação aos titulares e integração com a rotina das unidades, de modo a assegurar fluidez operacional e evitar impactos às atividades institucionais.
20.5. Adicionalmente, deverão ser adotadas providências de orientação aos usuários, com disseminação de boas práticas relativas ao uso, guarda e responsabilidade sobre os certificados digitais, mitigando riscos de uso indevido, compartilhamento irregular ou comprometimento de credenciais.
20.6. Por fim, recomendase a manutenção de registros gerenciais e relatórios periódicos, permitindo avaliação contínua da execução contratual, do consumo dos quantitativos previstos e da necessidade de ajustes ou planejamento de renovações futuras, assegurando transparência, controle e aderência ao planejamento institucional.

20.7. Providências operacionais (checklist para SEI/TR)

Etapa	Providência	Responsável	Prazo
Planejamento	Consolidar titulares/unidades e cronograma de emissão/renovação	Requisitante /TI	[ ]
Requisitos	Definir critério A1 vs A3 e casos “somente certificado”	Requisitante /TI	[ ]
TR	Elaborar TR com requisitos, SLA, suporte, reemissão/revogação e aceitação SSL OV	Requisitante /TI	[ ]
Execução	Organizar logística/agenda e infraestrutura para validação externa	Requisitante	[ ]
Fiscalização	Designar gestor/fiscal e rotinas de ateste/medição mensal	Autoridade	[ ]
Governança	Implantar controle de validade, revogações, reemissões e inventário de certificados	TI	[ ]

21. Declaração de Viabilidade

Esta equipe de planejamento declara **viável com restrições** esta contratação com base neste Estudo Técnico Preliminar.

21.1. Justificativa da Viabilidade com Restrições

A contratação é viável por existir demanda quantificada e precificada, por a solução atender requisitos de conformidade ICP Brasil e segurança web (SSL OV), e por o custo estimado ser compatível com o benefício institucional e com a necessidade de continuidade dos serviços digitais, permitindo gestão e fiscalização por medição mensal.

22. 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.

EDUARDO LIMA MACAMBYRA

Chefe de Divisão

Assinou eletronicamente em 07/03/2026 às 09:35:13.