ESTADO DE SANTA CATARINA
PODER JUDICIÁRIO

ESTUDO TÉCNICO PRELIMINAR

UNIDADE DEMANDANTE
Diretoria de Tecnologia da Informação – DTI.

I. DESCRIÇÃO DA NECESSIDADE PÚBLICA

I.1 Qual a necessidade pública?

Em observância às diretrizes estabelecidas na Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), aprovada pela Resolução n. 370/2021, vigente para o período de 2021 a 2026, e em consonância com os macro desafios do Poder Judiciário, especialmente no que se refere à infraestrutura e à governança de TIC, os novos sistemas de informação desenvolvidos devem oferecer suporte a assinaturas eletrônicas baseadas em certificados digitais emitidos por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Os sistemas que integram o processo de modernização do Poder Judiciário nacional demandam que o Magistrado ou o Servidor, assim como os documentos por eles produzidos, tenham sua autenticidade devidamente comprovada. Tal comprovação é assegurada por meio do uso de certificados digitais pessoais do tipo A3, os quais devem ser gerados e armazenados em dispositivos criptográficos apropriados, em conformidade com as normas da ICP-Brasil, instituída pela Medida Provisória n. 2.200-2.

Assim, a necessidade pública consiste em promover a segurança da informação no Poder Judiciário, validar a identidade institucional e garantir a criptografia de credenciais e senhas de acesso aos portais e sistemas do PJSC, bem como de sistemas de outros órgãos, promovendo a segurança dos portais e documentos digitais produzidos pelo Poder Judiciário.

I.2 Será uma contratação inédita?

Não será uma contratação inédita, porquanto a demanda já foi contemplada em processos anteriores, tais como nos SEI n. 0037939-09.2022.8.24.0710 e n. 0004487-37.2024.8.24.0710.

I.3 Como esta necessidade pública vem sendo atendida até o momento?

Em 21 de janeiro do corrente ano, a Seção de Apoio Administrativo/DSGA/DTI tomou conhecimento da rescisão do Contrato n. 27/2024, cuja rescisão unilateral é objeto do SEI n. 0088877-03.2025.8.24.0710. Diante da necessidade de continuidade do serviço, foi realizada contratação direta emergencial, conforme

SEI n. 0009400-91.2026.8.24.0710.

Posteriormente, a DTI sinalizou à DMP o interesse na consulta aos remanescentes do Pregão Eletrônico n. 90032/2024. A consulta foi realizada em 20/03/2026, restando fracassada, conforme registrado no SEI n. 0021064-22.2026.8.24.0710.

Diante do exposto, faz-se necessária a inclusão, no planejamento de contratações, de novo certame para atendimento da necessidade, considerando que o quantitativo adquirido por meio de contratação direta é insuficiente para atender à demanda anual. Informa-se, ainda, que, durante a fase de preparação do novo certame, será necessária a realização de nova contratação direta, em caráter emergencial, para assegurar a continuidade do fornecimento dos certificados digitais.

I.3.1 Qual o número do processo administrativo da contratação anterior?

A contratação anterior foi objeto dos processos administrativos ns. 0047800-82.2023.8.24.0710, 0003751-53.2023.8.24.0710, 0037939-09.2022.8.24.0710 e 0004487-37.2024.8.24.0710.

I.4 Em que data a contratação para o atendimento desta necessidade precisa estar vigente?

A contratação para o atendimento desta necessidade deve estar vigente em 07/11/2026.

II. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

II.1 - Identificação da demanda no PCA: DTI287.

II.2 - Identificação da demanda no PCSTIC: DTI287 - Aquisição de certificados digitais A3 (cadeia AC-Jus), em nuvem e em *token.*

Foi prevista a possibilidade de contratação compartilhada com outros órgãos, no caso de aquisição de bens por Sistema de Registro de Preços, conforme a Res. GP n. 02/2022?

() sim, razão pela qual podem ser consultados os órgãos públicos participantes dos Termos de Cooperação Técnica n. 47/2021 e n. 7/2024.

(x) não, pois se trata da contratação de serviços pelo regime de empreitada por preço unitário, e não de aquisição por registro de preços, não se enquadrando nas hipóteses da Resolução GP. n. 02/2022.

III. REQUISITOS DA CONTRATAÇÃO

III.1 Quais os requisitos da contratação

III.1.1 Requisitos técnicos

III.1.1.1 Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Justificativa: conforme previsão normativa MP 2.200-2.

III.1.1.2 Ser aderente ao Leiaute da Autoridade Certificadora da Justiça - AC-JUS

Justificativa: a AC-JUS é a primeira Autoridade Certificadora no mundo criada e mantida pelo poder judiciário. Foi criada após a edição da MP 2200-2/2001, institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, ou seja, assinados com certificados digitais emitidos dentro da hierarquia da ICP-Brasil.

O Conselho da Justiça Federal decidiu pela criação de uma Autoridade Certificadora para possibilitar a definição de regras e perfis de certificados, específicos para aplicações do Judiciário

III.1.1.3 Perfil: Pessoa Física.

Justificativa: conforme necessidade da Unidade Demandante.

III.1.1.4 Nível: A3.

Justificativa: conforme necessidade da Unidade Demandante.

III.1.1.5 Garantir a integridade, autenticidade e o não-repúdio dos atos praticados nos processos eletrônicos já disponibilizados aos Magistrados e Servidores do Poder Judiciário de SC (de forma segura e com validade jurídica).

Justificativa: conforme necessidade do Poder Judiciário de Santa Catarina para garantir autenticidade, integridade e não repúdio aos documentos digitais.

III.1.1.6 Garantir a continuidade de utilização do certificado digital para os casos em razão de mudança do estado civil.

Justificativa: primar pela economicidade ao reaproveitar a certificação digital em caso de mudança de estado civil.

III.1.1.7 Garantir a continuidade de utilização do certificado digital para os casos de perda, extravio, roubo, furto, sinistro ou defeito técnico na mídia.

Justificativa: primar pela economicidade ao reaproveitar a certificação digital em caso de perda, extravio, roubo, furto, sinistro ou defeito técnico na mídia.

III.1.1.8 Deve permitir sua utilização para assinatura de documentos eletrônicos, e-mails, autenticação de cliente e realizar logon na rede.

Justificativa: conforme necessidade do Poder Judiciário de Santa Catarina para garantir autenticidade, integridade e não repúdio aos documentos digitais.

III.1.1.9 Ser instalado em Token Criptográfico certificado pelo Instituto Nacional de Tecnologia da Informação – ITI.

Justificativa: a mídia de armazenamento tipo Token é a mais adequada por utilizar por USB 2.0, típica dos computadores do PJSC e possibilitar o transporte da certificação digital pelo usuário em mídia de armazenamento, em consonância a previsão normativa MP 2.200-2.

III.1.1.10 Armazenamento em nuvem

Justificativa: redução de tempo com instalação, configuração e suporte técnico de dispositivos físicos. Eliminação de problemas recorrentes de compatibilidade de drivers e portas USB. Permite assinatura digital

de qualquer dispositivo autorizado, sem necessidade de mídia física.

III.1.1.11 Quando constatada emissão imprópria ou defeituosa de um certificado, durante sua vigência, o mesmo deverá ser revogado e reemitido sem ônus à Contratante.

Justificativa: para garantir a utilização da certificação, conforme necessidade da Unidade Demandante.

III.1.1.12 Visitas técnicas para validação presencial nas dependências do edifício sede do TJ, na Academia Judicial, e nas demais unidades administrativas e judiciais situadas na Capital, a critério da contratante.

Justificativa: prestar o serviço de validação presencial do presidente do TJ, dos magistrados inscritos na formação inicial da magistratura bem como de outros magistrados e servidores, a critério da contratante.

III.1.2 Requisitos administrativos

III.1.2.1 Acesso a Ambiente Virtual Corporativo

Justificativa: viabilizar acompanhamento, por parte do TJSC, das solicitações, agendamentos, emissões, validades e outros atos pertinentes ao gerenciamento dos certificados digitais, além de permitir o upload da carta de autorização.

III.1.2.2: Possuir Autoridade de Registro em Florianópolis, num raio de 10 (dez) quilômetros da Sede do Tribunal de Justiça, com funcionamentos nos dias úteis, por no mínimo 3 (três) horas no período vespertino.

Justificativa: viabilizar atendimento presencial para os magistrados e servidores, a critério da contratante.

III.1.2.3: Apresentar atestado de capacidade técnica, expedido (s) por pessoa jurídica de direito público ou privado, que comprove a entrega de, pelo menos, 50% (cinquenta por cento) do solicitado, sendo permitido o somatório de atestados.

Justificativa: a exigência de comprovação de experiência prévia na emissão e entrega de certificados digitais especificamente da cadeia AC-JUS justifica-se pela natureza crítica das atividades do Poder Judiciário. A ICP-Brasil estabelece normas rigorosas para as diferentes cadeias de certificação, e a infraestrutura da AC-JUS possui particularidades de validação, níveis de segurança (A3/A4) e requisitos de integração com sistemas processuais (como PJe, e-Proc, e-STF, entre outros) que diferem das cadeias comerciais genéricas. A contratação de uma empresa sem expertise comprovada nessa cadeia específica traria um risco iminente de incompatibilidade técnica e interrupção das assinaturas de magistrados e servidores, gerando grave prejuízo à prestação jurisdicional.

A fixação do quantitativo mínimo de 50% (cinquenta por cento) guarda estrita proporcionalidade com a dimensão do contrato pretendido e com a necessidade da Administração de aferir a capacidade operacional e logística da licitante. Não se trata de restrição à competitividade, mas sim da aplicação do princípio da segurança, garantindo que a contratada possua estrutura capaz de gerenciar demandas de médio e grande porte (emissão, validação presencial ou por videoconferência, e entrega tempestiva), evitando que empresas sem fôlego operacional venham a dar causa à inexecução contratual.

III.1.3 Requisitos de sustentabilidade

Em conformidade com o Guia de Contratações Sustentáveis do Poder Judiciário de Santa Catarina.

III.1.3.1 Descarte sustentável ou reuso de ativos de TI: a certificação digital do PJSC, desde 2022, adota a reutilização de *token*, ou seu descarte sustentável, quando não possível o reuso. A tabela 1 (item 3.2) demonstra um decréscimo na aquisição dessa mídia.

Justificativa: a exigência de descarte sustentável ou reuso de ativos de TI justifica-se pelo alinhamento da contratação à Política de Sustentabilidade do Poder Judiciário de Santa Catarina (PJSC) e às diretrizes de

Governança de TI. Desde 2022, o PJSC adota o reaproveitamento de *tokens* ou a destinação ambientalmente adequada de mídias inservíveis. Como demonstrado na Tabela 1 (item 3.2), essa prática gerou um decréscimo real na necessidade de aquisição de novos insumos, comprovando a maturidade logística e a eficiência econômica do modelo. Portanto, o requisito visa a garantir que a empresa contratada possua processos homologados para absorver e operacionalizar essa rotina de reuso e descarte verde, evitando o desperdício de recursos públicos, mitigando o impacto ambiental do lixo eletrônico e assegurando a continuidade dos resultados já consolidados pela instituição.

III.1.3.2 Priorização de processos em forma eletrônica: toda a operação da certificação digital, desde a ordem de serviço até o recebimento das entregas e seu faturamento, deve ser realizada em meio digital e remoto, salvo casos excepcionais de validação presencial, quando o usuário não possuir requisitos para validação por videoconferência.

Justificativa: a exigência de priorização de processos em formato eletrônico justifica-se pela necessidade de manter o alinhamento da contratação com a transformação digital e a política de sustentabilidade do Poder Judiciário. Atualmente, todo o fluxo da operação — compreendendo desde a abertura da ordem de serviço até o recebimento das entregas e o faturamento — é executado de forma 100% digital e remota. As interações físicas restringem-se exclusivamente à validação presencial de usuários que não preenchem os requisitos regulamentares para o atendimento por videoconferência. Logo, o requisito é indispensável para garantir que a contratada possua infraestrutura tecnológica e processos internos compatíveis com essa dinâmica desmaterializada, assegurando celeridade na tramitação administrativa, redução do uso de papel, rastreabilidade dos atos e eficiência logística na prestação dos serviços.

III.1.3.3 O suporte à certificação digital, em todas as fases, desde a validação, instalação, incluindo a correção de erros ou o saneamento de dúvidas, deverá ser prestado remotamente, tanto pelas equipes de suporte de informática do PJSC, quanto pelo suporte da contratada.

Justificativa: a previsão de suporte técnico remoto compartilhado justifica-se pela necessidade de garantir uma estrutura de atendimento ágil, integrada e descentralizada para os usuários do Poder Judiciário. Como a operação da certificação digital ocorre de ponta a ponta em ambiente digital, o suporte remoto — atuando desde a validação e instalação até a resolução de erros e dúvidas — otimiza o tempo de resposta e elimina custos com deslocamentos. A atuação coordenada entre as equipes de informática do PJSC e o suporte da contratada garante um modelo de atendimento em camadas, onde incidentes básicos são triados internamente e problemas complexos são escalados diretamente ao fornecedor. Assim sendo, o requisito é essencial para assegurar a continuidade dos serviços, exigindo da contratada canais de atendimento e pessoal técnico qualificado para atuar de forma remota e cooperativa com a estrutura de TI do Tribunal.

III.2 Quais as justificativas para os requisitos escolhidos?

Conforme item III.1.

III.3 Quais normas devem ser atendidas para que a solução alcance seus objetivos?

Respeito às normas instituídas na Política Nacional de Resíduos Sólidos – PNRS (Lei n. 12.305/2010) e priorização de soluções que contemplem logística reversa e reciclagem e reaproveitamento de materiais, além da observância à Lei n. 11.419/2006 e à MP n .2.200-2.

IV. ESTIMATIVAS DE QUANTIDADE

IV.1 Quantas unidades de serviços ou bens deverão ser contratadas?

A demanda infere:

Item 1 – Certificados digitais A3 - pessoa física - cadeia ACJus - vigência 36 meses – sem limite de acessos/assinaturas - em nuvem - **1400 unidades**. CAT/SERV: 485464.

Item 2 – Certificados digitais A3 - pessoa física - cadeia ACJus - vigência 36 meses - para *token* (apenas o certificado digital) - **300 unidades**. CAT/SERV: 27219 ou 485464.

Item 3 – Visitas técnicas para validação presencial, emissão e gravação do certificado digital - **200 unidades**. CAT/SERV: 484744.

IV.2 Qual o histórico da demanda pelo bem ou serviço?

Ano	**Certificado Digital**	***Token****
2019	2506	2506
2020	2088	2088
2021	817	817
2022	1602	918
2023	1535	313
2024	804	196
2025	1055	132

Tabela 1: quantitativo de certificados digitais e de *tokens* fornecidos entre 2019 e 2025.

*A partir de 2022, com o Contrato n. 15/2022 (0020057-34.2022.8.24.0710), passou-se a adotar dois tipos de contratação: (a) certificados digitais com fornecimento de novo *token*, destinados aos usuários que não possuíam a mídia, e (b) certificados digitais para uso em *token* já existente, sem fornecimento de novo dispositivo, em razão da adoção da validação remota. Com essa mudança, o usuário deixou de precisar se deslocar até uma Autoridade de Registro (AR) para emissão do certificado, passando a reutilizar o token já disponível. Contudo, a entrega da mídia permanecia sob responsabilidade da empresa contratada, o que ainda exigia o deslocamento do usuário até uma AR para retirada do *token*.

Em 2023, houve nova alteração no objeto da contratação, com a separação das aquisições em dois itens: (a) *tokens*, que passaram a ser mantidos em estoque pela DTI e pelos setores de suporte de informática de todas as unidades do PJSC, e (b) certificados digitais, sem fornecimento de *token* (Contrato n. 8/2023, SEI 0003751-53.2023.8.24.0710).

Essa solução mostrou-se mais eficiente, pois conferiu à DTI total controle sobre a distribuição dos *tokens*, enquanto a emissão dos certificados digitais passou a ocorrer de forma totalmente remota.

Esse novo modelo explica a redução no consumo de *tokens*: das 1.500 unidades adquiridas em 2023, menos

da metade foi efetivamente utilizada desde então.

IV.3 Haverá incremento ou diminuição da demanda levando-se em conta os objetivos propostos no Planejamento Estratégico Institucional ou no planejamento específico da unidade gestora orçamentária, a exemplo do Plano de Obras ou Plano Diretor de Tecnologia da Informação?

Não é possível estimar incremento ou diminuição do consumo, considerando que novos sistemas podem ser adotados por este PJSC, ou por todo o Poder Judiciário do País, e trazer consigo esta necessidade.

Gestores de sistemas em uso hoje podem modificar as regras e determinar a adoção do uso da certificação digital para aumentar a segurança.

IV.4 Haverá fixação de quantidade mínima por pedido, em caso de aquisição de bens?

Não se aplica, pois não se trata de aquisição de bens.

IV.4.1 Qual a justificativa caso não se indique quantidade mínima por pedido?

Atendimento daquelas situações marcadas pela imprevisibilidade, seja no que tange ao quantitativo e/ou ao momento em que se farão necessárias as efetivas contratações.

A demanda de certificados digitais é imprevisível, pois não está apenas galgada no histórico de consumo e no vencimento de licenças. Além destas, outras variáveis tornam a estimativa de consumo imprevisível, tais como perdas, extravios e furtos, o ingresso de novos magistrados, servidores que passam a exercer atividades que necessitam certificados digitais, alteração de normativas acerca de documentos eletrônicos, entre outras. Nesse sentido, as quantidades indicadas nesse estudo consideraram empiricamente a influência dessas variáveis no histórico de consumo de certificações digitais, de acordo com a equipe da Seção de Apoio Administrativo da Divisão de Suporte e Gestão de Ativos de TI da DTI.

V . SOLUÇÕES DISPONÍVEIS NO MERCADO e ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

A certificação digital no padrão e-CPF A3, emitida na cadeia de confiança Cert-JUS da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), constitui requisito obrigatório para o exercício de atribuições institucionais por magistrados
e servidores do Poder Judiciário de Santa Catarina, para assegurar a autenticidade, integridade e validade jurídica de atos no meio digital no âmbito do Poder Judiciário de Santa Catarina (PJSC).

A ICP-Brasil opera sob um modelo de raiz única, no qual o Instituto Nacional de Tecnologia da Informação (ITI) atua como Autoridade Certificadora Raiz (AC-Raiz), sendo responsável pelo credenciamento, supervisão e auditoria
das demais entidades da cadeia hierárquica, composta pelas Autoridades Certificadoras (ACs) e pelas Autoridades de Registro (ARs).

No contexto da cadeia Cert-JUS, apenas ACs credenciadas especificamente para atuar no âmbito do PJSC estão habilitadas a emitir os certificados digitais institucionais. Atualmente, de acordo com consulta realizada ao portal oficial da AC-JUS, encontram-se credenciadas as seguintes Autoridades Certificadoras:

- AC Certisign JUS;

- AC Serasa-JUS;

- AC Serpro-JUS;

- AC Soluti-JUS;

- AC Valid-JU; e

- AC Safeweb-JUS.

Estas ACs operam por meio de redes de Autoridades de Registro (ARs), que assumem a interface com os usuários finais e executam as etapas de conferência documental, validação dos dados, identificação presencial ou remota e emissão ou renovação dos certificados digitais.

Diante desse cenário, foram mapeadas duas soluções possíveis para o atendimento à demanda do Poder Judiciário de Santa Catarina:

Solução 1: Contratação de serviços de validação, emissão e instalação de certificados digitais de pessoa física, A3, Cadeia AC-JUS, para instalação em *token* e armazenados em nuvem, incluindo visitas técnicas para validação presencial no município de Florianópolis/SC.

Justificativa: a imperiosa necessidade de garantir a continuidade das atividades finalísticas e administrativas do Poder Judiciário do Estado de Santa Catarina (PJSC), assegurando a magistrados e servidores os meios legais para a assinatura digital de atos e documentos com total validade jurídica, autenticidade, integridade e não-repúdio. Este modelo de prestação, amplamente adotado no âmbito da Administração Pública, supre de forma eficaz e continuada a demanda por certificados digitais no PJSC há mais de uma década, dispensando investimentos estruturais em pessoal, equipamentos ou infraestrutura tecnológica. Ademais, as empresas certificadoras credenciadas seguem padrões rigorosos de conformidade estabelecidos pela ICP-Brasil, garantindo a segurança, a legalidade e a compatibilidade com os sistemas informatizados utilizados pelo PJSC.

Considerando a natureza do objeto que se pretende contratar e o teor das normas atinentes à certificação digital, especialmente a Lei n. 11.419/2006 sobre o processo digital e a MP n. 2.200-2 que institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil como ente responsável pela autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras, constata-se que não há outras soluções tecnológicas para o fornecimento de certificação digital disponíveis no mercado que sejam compatíveis com os parâmetros legais, normativos e de interoperabilidade requeridos para o funcionamento pleno das atividades do PSJC.

Descrição, considerando o ciclo de vida da solução: A solução apresenta um ciclo de vida híbrido e de transição tecnológica, estruturado nas seguintes etapas:

a) Planejamento e Alocação: Identificação do perfil do usuário para direcionamento à modalidade adequada (preferencialmente Nuvem, mantendo o *Token* Físico como exceção justificada).

b) Validação de Identidade: Realizada presencialmente em Florianópolis/SC, caso necessário, por meio de visita técnica *in loco* (ou por videoconferência nas hipóteses regulamentares), onde é feita a coleta biométrica e verificação de documentos.

c) Emissão e Ativação: Conforme o perfil, o par de chaves criptográficas é gerado e instalado na mídia física (*Token* USB) ou ativado no ambiente seguro de Nuvem (HSM) da Autoridade Certificadora.

d) Fase de Utilização: Suporte técnico continuado para garantir a compatibilidade com os sistemas processuais do Judiciário (como e-Proc e PJ-e).

e) Encerramento do Ciclo e Renovação: Ao término da validade do certificado (geralmente em 36 meses), o usuário realiza a renovação migrando para o armazenamento em nuvem. Nesse momento, o ciclo de vida da mídia física se encerra, acionando a etapa de descarte ecológico e logística reversa dos *tokens* obsoletos, reduzindo progressivamente a pegada de resíduos eletrônicos do órgão.

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? Sim. O modelo híbrido de contratação (*Token* + Nuvem) para a cadeia AC-JUS é o padrão adotado atualmente pelos principais órgãos do Poder Judiciário nacional, a exemplo do Tribunal Regional Federal da 4ª Região (TRF4) e de Tribunais Regionais do Trabalho (TRTs). Esses órgãos utilizam soluções integradas de grandes Autoridades Certificadoras (como Certisign, Soluti, AC Serpro-JUS e Valid) para garantir que magistrados e servidores mantenham a interoperabilidade tanto em sistemas legados quanto em plataformas móveis de nova geração.

A Solução é aderente às regulamentações da ICP-Brasil? Sim. Ambas as modalidades de armazenamento propostas (*Token* Criptográfico e Nuvem) cumprem integralmente as resoluções e normas técnicas vigentes do Comitê Gestor da ICP-Brasil para a categoria de certificados tipo A3. A solução em nuvem utiliza Prestadores de Serviço de Confiança (PSC) devidamente homologados, assegurando idêntico valor jurídico, autoria, integridade e não-repúdio em relação às mídias físicas tradicionais.

Valor estimado considerando o ciclo de vida da solução: O valor estimado deve considerar a soma dos custos individuais de cada modalidade e os serviços logísticos locais, consoante se depreende da pesquisa de preços abaixo (docs. 10722232, 10763516, 10763534 e 10763561):

PESQUISA DE PREÇOS

Item 1 – Certificados digitais A3 - pessoa física - cadeia ACJus - vigência 36 meses - sem limite de acessos/assinaturas - em nuvem - **1400 unidades**. CAT/SERV: 485464.

EMPRESA	DATA	PREÇO
Fornecedor A	03/06/2026	R$ 324,40
Fornecedor B	08/06/2026	R$ 410,00
Fornecedor C	08/06/2026	R$ 310,00
PREÇO MÉDIO		**R$ 348,133**

Fonte da pesquisa de mercado: Cotações diretas de mercado junto às Autoridades Certificadoras credenciadas pela ICP-Brasil e operantes na região de Florianópolis/SC

Item 2 – Certificados digitais A3 - pessoa física - cadeia ACJus - vigência 36 meses - para token (apenas o certificado digital) - **300 unidades**. CAT/SERV: 27219 ou 485464.

EMPRESA	DATA	PREÇO

Fornecedor A	03/06/2026	R$ 210,00
Fornecedor B	08/06/2026	R$ 240,00
Fornecedor C	08/06/2026	R$ 310,00
PREÇO MÉDIO		**R$ 253,333**

Fonte da pesquisa de mercado: Cotações diretas de mercado junto às Autoridades Certificadoras credenciadas pela ICP-Brasil e operantes na região de Florianópolis/SC

Item 3 – Visitas técnicas para validação presencial, emissão e gravação do certificado digital - **200 unidades**. CAT/SERV: 484744.

EMPRESA	DATA	PREÇO
Fornecedor A	03/06/2026	R$ 1.594,00
Fornecedor B	08/06/2026	R$ 500,00
Fornecedor C	08/06/2026	R$ 0,50
PREÇO MÉDIO		**R$ 698,166**

Fonte da pesquisa de mercado: Cotações diretas de mercado junto às Autoridades Certificadoras credenciadas pela ICP-Brasil e operantes na região de Florianópolis/SC

No Brasil, o ecossistema do Poder Judiciário está em plena transição para o modelo de certificação digital em nuvem. A adoção varia entre os tribunais, dividindo-se entre aqueles que já utilizam a nuvem corporativamente para seus magistrados e servidores, e a compatibilidade dos sistemas processuais (como PJe, e-Proc e e-SAJ) para que advogados e defensores externos também possam peticionar usando essa tecnologia.

Os principais tribunais e ramos do Judiciário que já adotam ou estão homologando o modelo em nuvem incluem o Superior Tribunal de Justiça (STJ), o Conselho Nacional de Justiça (CNJ), o Tribunal Regional do Trabalho da 2ª Região (TRT-2, São Paulo), o Tribunal Regional do Trabalho da 3ª Região (TRT-3, Minas Gerais), o Tribunal Regional do Trabalho da 4ª Região (TRT-4, Rio Grande do Sul) e o Tribunal Regional do Trabalho da 9ª Região (TRT-9, Paraná), bem como o Tribunal Regional Federal da 3ª Região (TRF-3) e o Tribunal Regional Federal da 4ª Região (TRF-4), além de vários Tribunais de Justiça Estaduais, tais como TJ-PB (Paraíba), TJ-SP (São Paulo) e TJ-RS (Rio Grande do Sul).

Solução 2: Constituir o PJSC em Autoridade de Registro (AR) para emissão de certificado da cadeia AC-JUS em *token* e em nuvem.

A segunda solução analisada refere-se à possibilidade de estruturação institucional do PJSC como Autoridade de Registro (AR), vinculada a uma das ACs da cadeia Cert-JUS, assumindo diretamente a responsabilidade pelas etapas de validação e emissão de certificados digitais. Embora tecnicamente possível, essa alternativa demanda planejamento de longo prazo, regulamentação interna, aquisição de equipamentos homologados, infraestrutura tecnológica, contratação ou capacitação de equipe dedicada, e manutenção de padrões rígidos de segurança e auditoria. Também implicaria custos fixos adicionais e riscos operacionais relevantes, sem garantia de retorno proporcional em termos de eficiência ou economicidade.

Justificativa: A análise desta solução fundamenta-se na busca por autonomia institucional na gestão de identidades digitais. Contudo, sua escolha desvia-se do foco da atividade-fim do Poder Judiciário do Estado de Santa Catarina, convertendo o Poder Judiciário de Santa Catarina em um ente estritamente operacional da infraestrutura de chaves públicas.

A rejeição desta alternativa justifica-se pelos seguintes fatores críticos:

- Inviabilidade Operacional e Desvio de Foco: a constituição de uma AR exige uma estrutura administrativa e técnica dedicada exclusivamente a auditar, validar e emitir certificados sob as regras estritas da ICP-Brasil. O deslocamento de servidores ou a contratação de pessoal exclusivo para essa função não se alinha à eficiência administrativa, visto que o mercado privado já oferece essa prestação de serviço de forma consolidada e competitiva.

- Alto Impacto Financeiro e Logístico: ao contrário da contratação de serviços terceirizados (onde o custo é sob demanda ou por licença consumida), tornar-se uma AR impõe ao PJSC custos fixos elevados e permanentes. Isso inclui a aquisição de estações de trabalho homologadas e com blindagem de segurança, sistemas de CFTV específicos para salas de validação, cofres, além do custeio de auditorias anuais obrigatórias e independentes.

- Riscos de Responsabilidade Civil e Administrativa: como Autoridade de Registro, o PJSC assumiria formal e juridicamente os riscos decorrentes de eventuais falhas na identificação de usuários, fraudes ou vazamento de chaves privadas. Qualquer inconformidade detectada pelo Comitê Gestor da ICP-Brasil ou pelo Instituto Nacional de Tecnologia da Informação (ITI) poderia resultar em sanções administrativas, suspensão das atividades de emissão e prejuízos diretos à prestação jurisdicional.

- Barreira de Transição Tecnológica: conforme a diretriz estratégica do órgão de migrar os usuários para certificados armazenados em nuvem e extinguir progressivamente as mídias físicas, o investimento na criação de uma infraestrutura física própria de AR nasce na contramão dessa modernização, gerando o risco de obsolescência precoce dos ativos adquiridos.

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? Não de forma preferencial ou generalizada. Embora historicamente alguns raros órgãos de grande porte da Administração Pública ou do Poder Judiciário (como o Tribunal de Justiça do Rio de Janeiro - TJRJ) tenham se constituído como Autoridade de Registro (AR) própria no passado, a tendência atual de mercado e de governança pública caminha no sentido oposto. Atualmente, a quase totalidade dos órgãos públicos e tribunais rejeita este modelo. Essas entidades optam por não assumir a estrutura de uma AR própria devido à alta complexidade regulatória da ICP-Brasil, exigência de instalações físicas blindadas com segurança avançada, custos elevados com auditorias anuais obrigatórias e desvio da atividade-fim do órgão. Também exigiria o desvio de servidores para atividades-meio, o que comprometeria a força de trabalho já reduzida da instituição, especialmente em um cenário de restrições orçamentárias e déficit de pessoal. Portanto, a prática consolidada e eficiente na Administração Pública contemporânea é a terceirização dessas etapas operacionais (validação e emissão) por meio de empresas credenciadas (Solução 1), restando a constituição de AR própria como uma alternativa em obsolescência e financeiramente desvantajosa para o PJSC.

A Solução é aderente às regulamentações da ICP-Brasil? Sim, potencialmente aderente, porém sob condições de altíssima complexidade e custo regulatório. A estruturação do PJSC como uma Autoridade de Registro (AR) vinculada à cadeia AC-JUS encontra pleno amparo nas resoluções do Comitê Gestor da ICP-Brasil. Contudo, para obter e manter a conformidade legal e a homologação junto ao Instituto Nacional de Tecnologia da Informação (ITI), o Tribunal precisaria cumprir uma série de requisitos regulatórios rigorosos, tais como:

- Padrões de Segurança Física e Lógica: exigência de infraestrutura física dedicada, dotada de salas blindadas, controle de acesso biométrico, cofres para mídias criptográficas e sistemas de monitoramento por circuito fechado de TV (CFTV) operando 24/7 com regras rígidas de auditoria.

- Auditorias Anuais Obrigatórias: submissão do órgão a auditorias independentes periódicas para renovação do credenciamento e verificação do cumprimento das Normas de Segurança da ICP-Brasil.

- Segregação de Funções e Pessoal: treinamento, certificação técnica e dedicação exclusiva de servidores para atuarem como Agentes de Registro, sendo proibidos de acumular funções que gerem conflito de interesses com a atividade de validação biométrica e documental.

Portanto, embora a solução seja normativamente aderente, o esforço administrativo, jurídico e financeiro para se adequar e sustentar as constantes atualizações regulatórias da ICP-Brasil torna essa alternativa inviável quando comparada à contratação de um prestador de serviço que já possui toda essa estrutura homologada e auditada pelo mercado (Solução 1).

Valor estimado considerando o ciclo de vida da solução: inestimável de forma precisa no momento, mas com projeção de custo proibitivo e amplamente desfavorável. O cálculo do valor estimado para o ciclo de vida desta solução (considerando um horizonte padrão de 36 meses) não se limita ao custo das licenças dos certificados, mas exige a soma de investimentos estruturais complexos que seriam integralmente custeados pelo PJSC, tais como:

a) Investimento Inicial: custos com obras civis para adequação de salas de segurança, aquisição de mobiliário específico (cofres, portas de segurança), compra de estações de trabalho dedicadas e homologadas pela ICP-Brasil, e implantação de sistemas de monitoramento por CFTV de alta resolução com armazenamento de longo prazo;

b) Custos Operacionais Contínuos: custeio de auditorias externas independentes anuais, obrigatórias para a manutenção do credenciamento da AR junto ao ITI (Instituto Nacional de Tecnologia da Informação); pagamento de taxas de credenciamento e homologação junto à ICP-Brasil e à Autoridade Certificadora de nível superior; custo de oportunidade e folha de pagamento de servidores dedicados exclusivamente à função de Agentes de Registro (impedidos de atuar nas atividades-fim do tribunal); despesas com treinamentos, capacitações e certificações técnicas obrigatórias para a equipe; e

c) Custos de Desincorporação e Riscos: custos logísticos internos para coleta e descarte ecológico das mídias físicas obsoletas (tokens), além do provisionamento de risco financeiro por eventuais falhas operacionais ou fraudes de identificação sob responsabilidade da AR.

V.2 INDICAÇÃO SOBRE A NATUREZA DOS BENS (COMUM OU LUXO) APONTADOS NAS SOLUÇÕES DISPONÍVEIS

Não se aplica, considerando que se trata somente da contratação de serviços.

VI. JUSTIFICATIVA PARA PARCELAMENTO (CRITÉRIO DE ADJUDICAÇÃO)

VI.1 A adjudicação do objeto se dará por item ou por grupo de itens?

Os diversos itens que compõem o objeto são agrupados, conforme critérios previamente estabelecidos, de modo que apenas um licitante é o vencedor do grupo.

VI.2 Em caso de agrupamento de itens, quais as justificativas da não adoção do parcelamento da solução?

VI.2.1 Padronização tecnológica e compatibilidade

A adjudicação em lote único garante a padronização dos certificados digitais, cadeias de certificação,

softwares de gestão, drivers e procedimentos de validação, evitando problemas de incompatibilidade entre certificados de diferentes autoridades certificadoras, o que poderia comprometer a continuidade e a segurança dos serviços.

VI.2.2 Segurança da informação e integridade dos sistemas

A utilização de um único fornecedor reduz riscos relacionados à gestão de múltiplas infraestruturas criptográficas, assegurando maior controle sobre políticas de segurança, atualização de certificados, revogação e rastreabilidade, em conformidade com normas da ICP-Brasil e políticas internas de segurança da informação.

VI.2.3 Eficiência operacional e redução de complexidade

A contratação em lote único simplifica os processos de emissão, renovação, revogação e suporte técnico. Isso reduz a necessidade de múltiplos canais de atendimento, diferentes SLAs e treinamentos distintos, contribuindo para maior eficiência administrativa.

VI.2.4 Economia de escala e vantajosidade econômica

A adjudicação do conjunto dos certificados a um único licitante possibilita economias de escala, refletidas em melhores condições comerciais, preços unitários mais competitivos e redução de custos indiretos relacionados à gestão contratual, fiscalização e administração de múltiplos contratos.

VI.2.5 Racionalização da gestão contratual

A celebração de um único contrato reduz esforços de fiscalização, facilita o acompanhamento de prazos e metas, e diminui riscos de descumprimentos contratuais divergentes. Tal racionalização está alinhada ao princípio da eficiência administrativa.

VI.2.6 Continuidade do serviço e mitigação de riscos

A fragmentação da contratação entre diversos fornecedores pode gerar descontinuidade do serviço, especialmente em casos de falha, atrasos ou divergências técnicas entre prestadores. O lote único garante maior previsibilidade e responsabilidade integral do fornecedor sobre a execução contratual.

VI.2.7 Atendimento uniforme aos usuários finais

Um único fornecedor assegura tratamento uniforme aos usuários, com padrões consistentes de atendimento, prazos, procedimentos de identificação e suporte técnico, reduzindo reclamações e retrabalhos.

VI.2.8 Conformidade com o interesse público

A escolha pelo lote único está devidamente fundamentada em critérios técnicos, econômicos e operacionais, não tendo caráter restritivo indevido à competitividade, mas sim direcionada à obtenção da solução mais eficiente e segura para a Administração, em consonância com o interesse público.

VII. RESULTADOS PRETENDIDOS

VII.1 Benefícios diretos

VII.1.1 Segurança da informação: o certificado Tipo A3 utiliza dispositivos criptográficos seguros (token ou cloud HSM), reduzindo riscos de cópia, perda ou uso indevido; atende aos mais altos padrões da ICP-Brasil, com chaves privadas protegidas por hardware; e a cadeia AC-JUS é amplamente reconhecida no âmbito judicial, garantindo confiabilidade institucional.

VII.1.2 Validade jurídica e conformidade legal: as assinaturas com e-CPF têm pleno valor jurídico e permitem atuação segura em sistemas como PJe e e-Proc, CNJ, tribunais e sistemas governamentais, o que garante conformidade com normas de governança digital e controles internos.

VII.1.3 Continuidade operacional (serviço continuado): o modelo de contratação contínuo evita interrupções por vencimento de certificados, reduz riscos operacionais causados por atrasos em renovações ou emissão emergencial e facilita o planejamento administrativo e financeiro.

VII.1.4 Flexibilidade de uso: possibilita adequação a diferentes perfis de usuários e níveis de sensibilidade. Em nuvem: acesso remoto, mobilidade, ideal para teletrabalho e trabalho híbrido. Em *token* físico: opção para usuários que exigem controle local ou políticas mais restritivas.

VII.1.5 Validade estendida (36 meses): menor frequência de renovação reduz custos administrativos e retrabalho; mais estabilidade para usuários estratégicos; e melhor custo-benefício ao longo do ciclo contratual.

VII.2 Benefícios indiretos

VII.2.1 Redução de custos operacionais: diminuição do uso de papel, reconhecimento de firma, autenticações físicas e deslocamentos; menor demanda de suporte emergencial por expiração de certificados; e otimização da carga de trabalho das áreas administrativa e de TI.

VII.2.2 Aumento da Produtividade: assinaturas digitais rápidas e seguras agilizam processos internos e externos; redução do tempo de tramitação de documentos e processos judiciais/administrativos; e permite atuação simultânea e remota de diversos usuários.

VII.2.3 Padronização e governança: padroniza o uso de certificados digitais dentro da instituição; facilita auditorias, rastreabilidade e controle de responsabilidades; e contribui para maturidade digital e boas práticas de governança pública.

VII.2.4 Sustentabilidade e imagem institucional: redução significativa de papel e logística física; alinhamento com práticas de sustentabilidade e eficiência administrativa; e transmite modernidade, segurança e confiabilidade à sociedade.

VII.2.5 Escalabilidade e adaptabilidade: facilita inclusão de novos usuários sem reestruturações complexas; e ajusta-se a mudanças no volume de demandas ou evolução tecnológica.

VIII. PROVIDÊNCIAS PARA CELEBRAÇÃO DO INSTRUMENTO CONTRATUAL

VIII.1 Será necessário realizar capacitação de servidores para fiscalização e gestão contratual?

Não será necessário realizar capacitação de servidores para fiscalização e gestão contratual.

VIII.2 Será necessário realizar alguma adequação de ambiente para que o instrumento contratual possa ser celebrado?

Não será necessário realizar alguma adequação de ambiente para que o instrumento contratual possa ser celebrado.

IX. CONTRATAÇÕES CORRELATAS

IX.1 Será necessária alguma contratação interdependente para o início desta que será contratada?

Não haverá contratações interdependentes, nos termos do art. 18, § 1º, XI, da Lei n. 14.133/2021.

IX.2 Será necessária alguma contratação correlata a esta que será contratada?

Não haverá contratações correlatas, nos termos do art. 18, § 1º, XI, da Lei n. 14.133/2021.

X. IMPACTOS AMBIENTAIS e PRÁTICAS DE SUSTENTABILIDADE

X.1 Quanto aos critérios e práticas de sustentabilidade, preencher uma das seguintes alternativas

(x) Esta licitação possui item com critério de sustentabilidade indicado como requisito sustentável (item III.1.3);

( ) Apesar de haver critérios de sustentabilidade, optou-se por não adotá-los; e

( ) Não há critérios de sustentabilidade.

A contratação possui baixo impacto ambiental, posto tratar-se, basicamente, de serviço de validação e emissão de certificado digital.
As mídias permanecem sob responsabilidade dos usuários que são apresentados à educação socioambiental promovida pela Secretaria de Gestão Socioambiental do Tribunal de Justiça de Santa Catarina acerca do descarte adequado de resíduos.
O Poder Judiciário de Santa Catarina possui contrato de destinação ecológica de lixo eletrônico em consonância com a legislação ambiental vigente.
Atualmente, os usuários reutilizam os *tokens*. No entanto, com a inovação de contratar o certificado em

nuvem, a mídia física deixará de ser utilizada nas novas emissões, salvo pouquíssimas exceções. À medida que as renovações para o armazenamento em nuvem ocorrerem, os *tokens* obsoletos receberão o descarte ecológico já mencionado.

X.1.1 Qual a justificativa da não adoção de critérios de sustentabilidade ou de não haver critérios de sustentabilidade?

Item prejudicado, porquanto existem critérios de sustentabilidade.

X.2 Houve consulta ao Guia de Contratações Sustentáveis do PJSC pelos integrantes da Equipe de Planejamento da Contratação?

Sim, houve consulta ao Guia de Contratações Sustentáveis do PJSC pelos integrantes da Equipe de Planejamento da Contratação.

XI. DESCRIÇÃO DA SOLUÇÃO QUE MELHOR ATENDE À NECESSIDADE PÚBLICA

Contratação de serviços continuados de validação e emissão de Certificado Digital Tipo A3 (e-CPF), cadeia AC-JUS, com validade de 36 meses, em nuvem e em *token*, para execução no regime de empreitada por preço unitário, com a finalidade de manter o fornecimento de certificados digitais, a fim de assegurar a autenticidade, a integridade e o não repúdio dos documentos digitais produzidos pelo Poder Judiciário de Santa Catarina.

XII. ADEQUAÇÃO DO OBJETO À NECESSIDADE

Embora a constituição de Autoridade de Registro própria ofereça total controle sobre o fluxo de validação (Solução 2), a relação custo-benefício mostra-se amplamente desfavorável. O modelo de contratação de serviços terceirizados especializados (Solução 1) apresenta-se como a escolha técnica e economicamente vantajosa, pois transfere os riscos operacionais ao mercado, desonera a força de trabalho interna e garante o descarte ecológico das mídias obsoletas sem onerar a estrutura do PJSC.

Tal modelo dispensa a realização de investimentos em infraestrutura tecnológica, aquisição de equipamentos, mobilização de equipe técnica ou implantação de processos administrativos internos complexos, mantendo a solução já consolidada e funcional no âmbito do PJSC há mais de uma década. Trata-se, portanto, de uma alternativa que garante resposta célere, segura e padronizada, com execução sob demanda, o que mitiga riscos de descontinuidade e assegura flexibilidade na gestão do contrato.

Ressalta-se, ainda, que as empresas certificadoras credenciadas pela cadeia Cert-JUS estão submetidas a rígido controle de conformidade e auditoria pelo Instituto Nacional de Tecnologia da Informação – ITI, assegurando elevados padrões de qualidade, segurança e aderência às normas da ICP-Brasil.

O certificado digital do tipo A3 pode ser armazenado em três modalidades atualmente disponíveis no mercado: (i) cartão inteligente (smartcard); (ii) t*oken* USB; e (iii) nuvem. A escolha entre essas mídias deve observar critérios técnicos,
operacionais, econômicos e de compatibilidade com os sistemas utilizados pela Administração.

O cartão inteligente, embora ainda previsto nos normativos da ICP-Brasil, apresenta obsolescência tecnológica e baixa confiabilidade operacional. Sua fragilidade física, a necessidade de leitoras específicas com interface USB e sua

descontinuidade comercial inviabilizam sua adoção. Ressalta-se que sequer foi possível levantar cotações válidas para esse item, o que confirma sua retirada do mercado.

O token USB, por sua vez, constitui atualmente a solução mais consolidada no serviço público. Trata-se de uma mídia criptográfica portátil, amplamente compatível com os equipamentos utilizados no Tribubal, resistente, reutilizável, de baixo custo unitário e de fácil operação. Seu uso é tradicional no PJSC, inclusive com estrutura de suporte técnico e instruções já padronizadas. Além disso, a possibilidade de reaproveitamento nas renovações contribui para a redução de custos ao longo do tempo.

A certificação digital em nuvem representa uma alternativa mais recente e tecnológica, que elimina a necessidade de dispositivos físicos. Nessa modalidade, o acesso ao certificado é realizado mediante autenticação em múltiplos fatores (MFA), com uso de aplicativo autenticador instalado em dispositivos móveis do usuário. A geração temporária de senhas dinâmicas (OTP), com expiração a cada poucos segundos, proporciona elevado nível de segurança, mitigando riscos de acesso não autorizado e problemas decorrentes do esquecimento ou bloqueio de senhas fixas.

Além das vantagens em termos de segurança, a certificação em nuvem oferece ganhos de eficiência administrativa, com eliminação de custos com aquisição de mídias físicas e redução significativa de chamados técnicos por problemas com senhas ou dispositivos danificados.
Entretanto, a adoção do modelo em nuvem ainda se encontra em fase de transição no PJSC, havendo limitações técnicas e institucionais que restringem sua aplicação ampla e imediata. Destacam-se, entre os desafios, a necessidade de instalação de aplicativos autenticadores nos dispositivos móveis pessoais de magistrados e servidores e eventuais incompatibilidades com sistemas internos legados.

Diante desse contexto, opta-se pela contratação de serviços para emissão de certificados digitais em ambas as modalidades – *token* USB e nuvem – de forma complementar, de modo a garantir flexibilidade operacional e cobertura integral da demanda institucional.

Por meio destes estudos preliminares, concluiu-se que a solução escolhida (Solução 1), qual seja, a contratação de serviços continuados de validação e emissão de Certificado Digital Tipo A3 (e-CPF), cadeia AC-JUS, com validade de 36 meses, em nuvem e em *token*, mostra-se ser a que melhor atende à necessidade pública, uma vez que a certificação digital em nuvem representa evolução tecnológica em relação aos modelos baseados em mídia física, destacando-se as seguintes vantagens:

a) mobilidade: acesso remoto a partir de qualquer local e dispositivo conectado à internet;

b) eliminação de dispositivos físicos: dispensa uso de token, reduzindo risco de perda ou dano;

c) praticidade operacional: ausência de necessidade de instalação de drivers e softwares locais;

d) uso multiplataforma: funcionamento em computadores, tablets e smartphones;

e) agilidade nos processos: assinatura digital remota e imediata de documentos;

f) gestão centralizada: controle de uso, histórico de acessos e funcionalidades administrativas;

g) segurança avançada: utilização de autenticação multifator (ex.: senha e validação via dispositivo móvel);

h) redução de custos indiretos: eliminação de aquisição e manutenção de hardware criptográfico; e

i) alinhamento com tendências de mercado: modelo aderente ao cenário de transformação digital e trabalho remoto.

Além disso, a solução está devidamente adequada às necessidades da Unidade Demandante, bem como ao atendimento dos requisitos elencados no Termo de Abertura do Processo de Contratação.

Por fim, identificou-se que a adoção da solução proposta, sob os aspectos da eficácia, eficiência, economicidade e padronização, atinge os seguintes benefícios:

a) assegurar a continuidade e a manutenção dos serviços que utilizam certificados digitais, com elevados

níveis de desempenho, qualidade e confiabilidade;

b) garantir a integridade, a autenticidade e o não repúdio das transações eletrônicas realizadas no âmbito do PJSC;

c) assegurar a segurança das informações trafegadas por meio dos acessos às aplicações disponibilizadas pelo PJSC; e

d) garantir a segurança no acesso aos portais institucionais do PJSC.

Destaca-se que a Diretoria de Tecnologia da Informação tem investido esforços no estudo da viabilidade da adoção do certificado digital em nuvem, de forma que, em poucos anos, mesmo a mídia física se tornará obsoleta.

A previsão de certificação digital em nuvem na presente contratação decorre do atual estágio de evolução tecnológica da Diretoria de Tecnologia da Informação (DTI), que já opera com soluções em ambiente de nuvem e possui experiência prática na utilização desse modelo de certificação digital. Os testes realizados e o uso inicial em produção evidenciaram benefícios relacionados à mobilidade, eficiência operacional e segurança, consolidando a adoção dessa tecnologia como parte integrante da rotina institucional.

Dessa forma, a inclusão de certificados digitais em nuvem no objeto da licitação não se caracteriza mais como iniciativa prospectiva, mas como atendimento a uma demanda já existente e devidamente validada no âmbito do órgão.

Não obstante, considerando a necessidade de garantir a continuidade dos serviços, a compatibilidade com determinados sistemas e a mitigação de riscos operacionais, a contratação permanece estruturada em modelo híbrido, contemplando também certificados em mídia física (*token*). Essa abordagem permite à Administração manter flexibilidade operacional diante de cenários específicos que ainda requerem ou possam vir a requerer o uso de certificados físicos.

Adicionalmente, a configuração do modelo contratual visa a possibilitar o ajuste dinâmico entre as quantidades contratadas de cada tecnologia ao longo da vigência, conforme a evolução das necessidades institucionais. Com isso, busca-se assegurar a eficiência do gasto público, evitando tanto a aquisição excessiva de mídias físicas quanto eventuais limitações operacionais, garantindo equilíbrio contratual e aderência às práticas de governança e gestão de riscos em tecnologia da informação.

XIII. PLANO DE SUSTENTAÇÃO

O Plano de Sustentação para dar vazão a aquisição de certificados digitais implicará na análise e encaminhamento dos pedidos de usuários por parte da Seção de Apoio Administrativo da Divisão de Suporte e Gestão de Ativos de TI. Portanto, os recursos necessários à continuidade do negócio durante e após a aquisição já estão disponíveis conforme abaixo descrito.

XIII.1. RECURSOS NECESSÁRIOS À CONTINUIDADE DO OBJETO CONTRATADO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

XIII.1.1 Recursos Materiais

Não se aplica.

XIII.1.2 Recursos Humanos

Recurso: Na Seção de Apoio Administrativo da DSGA: dois servidores. Nas unidades judiciais e administrativas os Setores de Suporte em Informática prestam suporte para instalação dos certificados digitais, e mantém em guarda as mídias criptográficas (tokens) para fornecimento aos usuários autorizados.

Disponibilidade: Sim
Ações para obtenção do Recurso: não se aplica
Responsável: Seção de Apoio Administrativo / DSGA

XIII.2 ESTRATÉGIA DE CONTINUIDADE CONTRATUAL EM EVENTUAL INTERRUPÇÃO

XIII.2.1 Encerramento do contrato por parte da Contratada:
Ações para contingência - aquisição direta para aquisição de certificados digitais por meio de Requisição de Compra (RC)

Prazo: 20 (vinte) dias
Responsável: Seção de Apoio Administrativo / DSGA

Ações para contingência - iniciar novo processo de aquisição de STI por meio de licitação

Prazo: 40 (quarenta) dias
Responsável: Seção de Apoio Administrativo / DSGA

XIII.2.2 Término de vigência de contrato:
Ações para contingência - iniciar novo processo de aquisição de Solução de Tecnologia da Informação

Prazo: 70 (setenta) dias antes do encerramento do contrato
Responsável: Seção de Apoio Administrativo / DSGA

XIII.2.3 Interrupção total/parcial do serviço:
Ações para contingência - aquisição direta para aquisição de certificados digitais por meio de Requisição de Compra (RC)

Prazo: 20 (vinte) dias
Responsável: Seção de Apoio Administrativo / DSGA

XIII.3 AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

XIII.3.1 Término de vigência de contrato:
Ações preventiva - iniciar procedimento para renovação do contrato, respeitados os critérios de vantajosidade.

Prazo: 12 (doze) meses antes do encerramento do contrato

Responsável: Seção de Apoio Administrativo / DSGA

XIII.3.2 Término de vigência de contrato:
Ações para contingência - iniciar novo processo de aquisição de Solução de Tecnologia da Informação

Prazo: 12 (doze) meses antes do encerramento do contrato
Responsável: Seção de Apoio Administrativo / DSGA

XIII.4 ESTRATÉGIA DE INDEPENDÊNCIA DO PJSC COM RELAÇÃO À EMPRESA CONTRATADA

XIII.4.1 Como se dará a transferência de conhecimento tecnológico nos casos de contratação de desenvolvimento de softwares sob encomenda no mercado de TIC?

Não se aplica.

XIII.4.2 Quais são os direitos de propriedade intelectual e autorais da Solução de Tecnologia da Informação e Comunicação, inclusive sobre os diversos produtos gerados ao longo do contrato, tais como a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados? Justificar caso tais direitos sejam exclusivos da empresa contratada.

Não se aplica.

Documento assinado eletronicamente por **Thalia Krause Brina**, **Analista Administrativo**, em 30/06/2026, às 17:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Jéssica Aline Flores**, **Analista Jurídica**, em 30/06/2026, às 18:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Luciano Michels Rocha**, **Técnico Judiciário Auxiliar**, em 01/07/2026, às 10:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Michelli Vieira Cherem**, **Chefe de Divisão**, em 02/07/2026, às 18:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Rafael Severo Roman**, **Chefe de Divisão**, em 03/07/2026, às 12:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjsc.jus.br/verificacao informando o código verificador **10845238** e o código CRC **CDECC6C9**.