



Estudo Técnico Preliminar

Processo Administrativo nº136/2026
CIA 0040881-31.2026.8.11.0000.

*Contratação de solução integrada de certificação digital padrão ICP-Brasil, para
atendimento das necessidades institucionais.*





Histórico de Revisões

Data	Versão	Descrição	Autor
08/07/2026	1.0	Rascunho da primeira versão do documento	Lorene Piccin
13/07/2026	1.1	Análise área técnica DSI	Thiago/ Jefferson/Paolla
14/07/2026	1.2	Revisão do documento - análise jurídica	Jean Barros
14/07/2026	1.3	Revisão do documento - Após revisão do Jean e Área Técnica	Lorene Piccin
21/07/2026	1.4	Análise Coordenação de TIC	Cleybson Sousa
10/08/2026	1.5	Análise Coordenadora de TIC	Marcia Buhr
24/08/2026	1.6	Análise área administrativa	Fábio e Moacyr
25/08/2026	1.7	Versão final para assinatura	Lorene Piccin





HISTÓRICO DE REVISÕES	2
1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO	5
1.1 CONTEXTUALIZAÇÃO	5
1.2 IDENTIFICAÇÃO DA DEMANDA NO PLANO DE CONTRATAÇÕES	7
1.3 CARACTERIZAÇÃO DA DEMANDA	8
1.3.1 DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES	8
1.3.2 DEFINIÇÃO E ESPECIFICAÇÕES DE REQUISITOS:	9
1.3.2.1 REQUISITOS FUNCIONAIS	9
1.3.2.2 REQUISITOS DE ARQUITETURA TECNOLÓGICA E COMPATIBILIDADE TÉCNICA	10
1.3.2.3 REQUISITOS DE CAPACITAÇÃO	11
1.3.2.4 REQUISITOS DE MANUTENÇÃO	12
1.3.2.5 REQUISITOS DE GARANTIA	13
1.3.2.6 REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO:	14
1.3.2.7 REQUISITOS DE EXPERIÊNCIA PROFISSIONAL E FORMAÇÃO DE EQUIPE	15
1.3.2.8 REQUISITOS TEMPORAIS	15
1.3.2.9 REQUISITOS DE SEGURANÇA E PRIVACIDADE	17
1.3.2.10 REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS	18
1.3.2.11 REQUISITOS LEGAIS	19
1.3.3 ADERÊNCIA A PADRÕES E MODELOS	20
1.3.3.1 MODELO NACIONAL DE INTEROPERABILIDADE - MNI	20
1.3.3.2 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP - BRASIL	21
1.3.3.3 MODELO DE REQUISITOS MOREQ-JUS	21
1.4 ATENDIMENTO DA DEMANDA	21
1.4.1 PORTAL DO SOFTWARE PÚBLICO BRASILEIRO	21
1.4.2 SOLUÇÕES DE TIC	22
1.4.3 CONTRATAÇÕES PÚBLICAS SIMILARES	23
1.4.4 SOLUÇÕES SIMILARES EM OUTROS ÓRGÃOS	24
1.4.5 MODELOS DE AQUISIÇÃO/PRESTAÇÃO DO SERVIÇO	24
1.4.6 CAPACIDADE E ALTERNATIVAS DO MERCADO DE TI	25
1.4.7 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES	26
1.5 ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA	26
1.6 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO	30
1.6.1 DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA	30





1.6.2	MOTIVAÇÃO DA ESCOLHA.....	31
1.6.2.1	CONTEXTO E JUSTIFICATIVA	31
1.6.3	BENEFÍCIOS ESPERADOS.....	35
1.6.4	RESULTADOS ESPERADOS	35
1.6.5	RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA	36
1.6.6	DA INTENÇÃO DE REGISTRO DE PREÇO	41
1.6.7	ESTIMATIVA DE CUSTO TOTAL DA SOLUÇÃO ESCOLHIDA	42
1.7	DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO	44
2.	SUSTENTAÇÃO DO CONTRATO	45
2.1	ADEQUAÇÃO DO AMBIENTE.....	45
2.2	DOS RECURSOS MATERIAIS E HUMANOS	46
2.3	CONTINUIDADE DO FORNECIMENTO	47
2.4	TRANSIÇÃO CONTRATUAL E ENCERRAMENTO DO CONTRATO	48
2.5	ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA.....	50
2.6	DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAIS	51
2.7	NÃO PARTICIPAÇÃO DE PESSOAS FÍSICAS CONSOANTE INSTRUÇÃO NORMATIVA SEGES/ME N. 116/2021:	51
3.	ESTRATÉGIA PARA A CONTRATAÇÃO	52
3.1	NATUREZA DO OBJETO.....	52
3.2	PARCELAMENTO E ADJUDICAÇÃO DO OBJETO	53
3.3	MODALIDADE E TIPO DE LICITAÇÃO	55
3.4	CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA	55
3.5	DAS IMPLICAÇÕES DA FORMA DE PAGAMENTO	56
3.6	VIGÊNCIA DOS BENS E/OU SERVIÇOS	56
3.7	EQUIPE DE APOIO À CONTRATAÇÃO.....	58
4.	ANÁLISE DE RISCOS	59
4.1	RISCOS MAPEADOS	60
5.	APROVAÇÃO E ASSINATURA	72
6.	CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC	73
	ANEXO A - LISTA DE POTENCIAIS FORNECEDORES	74
	ANEXO B - CONTRATAÇÕES SIMILARES.....	76
	ANEXO C – REQUISITOS TÉCNICOS	79
	ANEXO D – ORÇAMENTOS	88





ESTUDO TÉCNICO PRELIMINAR

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1 Contextualização

Atualmente, o Poder Judiciário do Estado de Mato Grosso é atendido pelo Contrato nº 128/2024, cujo objeto consiste na prestação de serviços de certificação digital para magistrados e servidores, contemplando a emissão de certificados digitais e o fornecimento de mídias criptográficas. O referido contrato possui vigência até 28 de agosto de 2027, sendo necessário iniciar o planejamento da nova contratação com antecedência suficiente para que a Administração possa avaliar as alternativas disponíveis no mercado, definir a solução mais adequada às necessidades institucionais e promover a transição para o novo modelo de certificação digital de forma planejada.

A certificação digital ICP-Brasil representa o pilar de validade jurídica, autoria e inviolabilidade de todos os atos praticados no Poder Judiciário do Estado de Mato Grosso. Os certificados digitais e-CPF (Cadeia Cert-JUS A3) atuam como a identidade lógica essencial para que magistrados e servidores realizem a assinatura eletrônica diária de petições, despachos, decisões e sentenças no PJe, além de garantirem o acesso seguro a sistemas críticos de apoio e plataformas governamentais.

Mais do que a mera manutenção de um contrato, a nova contratação promove a modernização e o ganho de eficiência da infraestrutura de assinatura digital do Tribunal. A introdução do modelo de certificação em nuvem (Cloud) — combinada à manutenção residual de tokens físicos — elimina a dependência exclusiva de hardwares, concede mobilidade total aos magistrados e servidores para assinarem atos processuais de qualquer dispositivo autorizado, e extingue os gargalos logísticos históricos de envio e substituição de mídias físicas no interior do Estado.

Dessa forma, a solução impacta diretamente a celeridade processual e a segurança da informação. Garantir a disponibilidade ininterrupta e moderna dos mecanismos de assinatura digital impede o represamento de minutas, o cancelamento de audiências virtuais e atrasos na prestação jurisdicional, assegurando ao cidadão um serviço público célere, confiável e alinhado à transformação digital do Judiciário.





Em decorrência das recentes diretrizes e normativas da ICP-Brasil para a cadeia Cert-JUS, cumpre registrar que as contratações do primeiro semestre ainda adotavam o prazo de validade de 30 (trinta) meses para os certificados digitais. Contudo, considerando que a partir de 25 de agosto de 2026 só serão emitidos e comercializados tokens e certificados com validade de até 24 (vinte e quatro) meses, faz-se necessária a readequação do prazo de vigência e da validade dos ativos da presente contratação para 24 meses. A medida visa otimizar o ciclo de vida útil criptográfico do ambiente e manter a estrita conformidade com a governança de TIC do Poder Judiciário.

A contratação contribuirá, ainda, para o fortalecimento da segurança da informação, para a conformidade com as normas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), da cadeia Cert-JUS e demais normativos aplicáveis, bem como para a ininterrupção e estabilidade da prestação jurisdicional eletrônica, reduzindo riscos de indisponibilidade dos serviços e assegurando maior confiabilidade aos processos eletrônicos desenvolvidos pelo Tribunal.

Por fim, a solução produzirá benefícios diretos à sociedade. Ao garantir a regularidade, a celeridade e a segurança da autenticação e das assinaturas eletrônicas realizadas por magistrados e servidores em todas as comarcas do Estado, mitigam-se os riscos de atrasos processuais, remarcações de audiências e indisponibilidades operacionais, assegurando a regularidade, a eficiência e a confiabilidade da prestação jurisdicional eletrônica oferecida ao cidadão.

1.1.1 Avaliação da Solução Atualmente Utilizada

A execução do Contrato nº 128/2024 permitiu identificar fragilidades operacionais, logísticas e de gestão que impactaram a eficiência do serviço e exigiram sucessivas intervenções corretivas do Departamento de Suporte e Informação. Esses diagnósticos fundamentam a necessidade de reestruturação dos requisitos para o novo certame, destacando-se:

- **Fragilidades na Logística de Distribuição:** Constatou-se a ocorrência de atrasos recorrentes no envio de mídias criptográficas às unidades solicitantes, além da necessidade atípica de o próprio Departamento de Suporte e Informação proceder ao envio de tokens





via Correios para evitar o desabastecimento das comarcas, evidenciando um desenho logístico ineficiente;

- **Qualidade e Padronização do Hardware:** Verificou-se a utilização e o fornecimento de tokens reaproveitados para o atendimento de novas demandas, em vez do fornecimento de dispositivos novos, impondo a necessidade de estabelecer critérios de qualidade e exclusividade de primeiro uso para os materiais disponibilizados;
- **Morosidade em Processos Administrativos:** Identificou-se lentidão na tramitação dos processos de pagamento devido ao atraso recorrente do atual fornecedor no envio das certidões de regularidade fiscal, exigindo o aperfeiçoamento dos mecanismos de gestão documental e cumprimento de prazos;
- **Alto Custo Operacional e de Deslocamento:** O modelo atual, excessivamente dependente da validação presencial e de mídias físicas, gera custos elevados com diárias e deslocamentos de usuários até os postos de atendimento, justificando a transição para o modelo em nuvem com validação remota por videoconferência;
- **Necessidade de Integração e Monitoramento:** Constatou-se a falta de um sistema integrado de gestão de chamados capaz de emitir relatórios de consumo e acompanhamento de SLAs, prejudicando a transparência e a fiscalização dos Indicadores de Medição de Resultados (IMR).

As inconformidades e oportunidades de melhoria identificadas na execução do contrato anterior fundamentam os requisitos técnicos, temporais e operacionais definidos neste Estudo Técnico Preliminar, servindo de diretriz para a elaboração do Termo de Referência e para a blindagem da futura execução contratual.

1.2 Identificação da demanda no Plano de Contratações

A Resolução nº 468/2022 determina que as contratações alçadas pelo Poder Judiciário do Estado de Mato Grosso estejam previstas no Plano de Contratações Anual,





com o objetivo de demonstrar a melhor forma de alocar recursos discricionários e alcançar os objetivos institucionais.

Em uma medida que reforça a transparência nas aquisições e gastos do PJMT, as informações do Plano de Contratações Anual para o ano de 2026 foram disponibilizadas, identificando a presente demanda conforme indicado abaixo:

Plano Anual de Contratações TIC – 2026: Esta ação está prevista no Plano Anual de Contratações de TIC 2026, no item E.14/Essencial, aprovado pelo Comitê de Governança de TIC, em 17/12/2025.

Além do Plano Anual de Contratações, será atendido o Planejamento Estratégico Institucional 2021-2026, e o Plano Diretor de Tecnologia da Informação e Comunicação:

- **Programa:** Programa de Transformação Digital.
- **Nome do Projeto:** Modernização de TIC no PJMT.
- **Objetivo Estratégico:** Fortalecer a estratégia e a infraestrutura de TIC, assegurando a transformação necessária ao negócio.
- **Justificativa:** Garantir a disponibilidade ininterrupta e a evolução da infraestrutura de certificação digital, assegurando aos magistrados, servidores e demais usuários autorizados o acesso seguro aos sistemas institucionais, a assinatura eletrônica de documentos e a realização célere de atos processuais e administrativos em meio digital.

1.3 Caracterização da demanda

1.3.1 Definição e Especificação das Necessidades

A presente contratação tem por objetivo atender às necessidades estratégicas, operacionais e de segurança do Poder Judiciário do Estado de Mato Grosso, estruturadas sob os seguintes eixos fundamentais de negócio e de tecnologia:

- **Necessidades de Negócio:** O PJMT necessita garantir que magistrados e servidores em todas as comarcas do Estado disponham de meios contínuos, válidos e ininterruptos de assinatura eletrônica para a prática de atos processuais





e administrativos. Adicionalmente, o negócio demanda o saneamento definitivo das fragilidades logísticas do Contrato nº 128/2024 (como atrasos na entrega de hardware e fornecimento de mídias reaproveitadas), transferindo a responsabilidade da distribuição expressa e suporte especializado integralmente ao mercado fornecedor.

- **Necessidades Tecnológicas:** O ambiente de TIC necessita evoluir a arquitetura atual para um modelo híbrido que incorpore a tecnologia de certificados digitais em nuvem, reduzindo gradativamente a dependência de ativos físicos. Tecnologicamente, faz-se indispensável assegurar o controle institucional sobre a geração de vouchers, criptografia baseada em HSMs seguros, conformidade restrita com a LGPD, os normativos do CNJ e a ICP-Brasil (Cadeia Cert-JUS), além de garantir auditabilidade total com o registro mandatório de cada chamado no sistema oficial de TI do órgão.

1.3.2 Definição e Especificações de Requisitos:

1.3.2.1 Requisitos Funcionais

Os requisitos funcionais devem conter:

- **Emissão e Modelagem Híbrida:** Disponibilização de serviços sob demanda para emissão, renovação, validação e revogação de certificados digitais do tipo e-CPF ICP-Brasil (Cadeia Cert-JUS A3), contemplando tanto o armazenamento em Nuvem (Cloud) quanto em mídia física (Tokens USB).
- **Gestão Centralizada (Vouchers):** Controle institucional do ciclo de vida dos certificados por meio da geração de vouchers numéricos estruturados e integrados, condicionados à prévia autorização da fiscalização do órgão.
- **Gerenciamento da Nuvem:** A solução em nuvem deve permitir ao titular o gerenciamento, a revogação instantânea e o compartilhamento temporário ou restrito do acesso a terceiros a partir de múltiplos dispositivos institucionais ou pessoais autorizados, sem que isso compute novas emissões.





- **Rastreabilidade Geral:** Vinculação obrigatória de todos os atendimentos, agendamentos, validações remotas por videoconferência (via Microsoft Teams ou plataforma indicada) e protocolos de envio logístico à ferramenta oficial de gestão de chamados do Tribunal.

1.3.2.2 Requisitos de Arquitetura Tecnológica e Compatibilidade Técnica

Os requisitos de arquitetura e compatibilidade técnica devem conter:

- **Padrão Criptográfico Mínimo:** Utilização de chaves criptográficas RSA de 2048 bits ou superior (ou padrão equivalente homologado pela ICP-Brasil), funções de resumo criptográfico SHA-256 ou superior, e algoritmos de assinatura digital compatíveis com as normas vigentes, tais como *sha256WithRSAEncryption* e *sha512WithRSAEncryption*.
- **Custódia Segura das Chaves Privadas - Nuvem:** No modelo de certificado em nuvem (cloud), as chaves privadas deverão ser geradas e armazenadas em ambientes criptográficos baseados em Hardware Security Modules (HSMs) com certificação mínima FIPS 140-2 ou superior, dotados de proteção física contra violação e detecção de acessos indevidos, sendo vedada sua exportação ou cópia local.
- **Proteção Física e Lógica (Mídia Criptográfica):** Para os certificados baseados em tokens USB, os dispositivos fornecidos devem possuir memória interna segura e não exportável, com certificação FIPS 140-2 ou superior, gerando as chaves exclusivamente dentro do próprio dispositivo.
- **Controle de Acesso e Autenticação Forte:** A infraestrutura de acesso ao certificado deve impor autenticação forte e multifator (MFA), combinando o uso de senhas/PIN com biometria facial, digital, tokens lógicos ou aplicativos autenticadores seguros,





associados a uma política de bloqueio automático após tentativas inválidas consecutivas.

- **Canais de Comunicação Protegidos:** Todo o tráfego de rede e comunicações realizadas entre usuário, aplicação, plataforma de assinatura e barramento de auditoria deverão ocorrer obrigatoriamente por canais criptografados via protocolo TLS 1.2 ou superior.
- **Mecanismos de Integração:** A solução deverá disponibilizar formas de integração técnica preservando a segurança da chave privada, por meio de bibliotecas configuráveis padrão PKCS#11, MSCAPI/CSP (integração nativa do Windows) ou mecanismo tecnicamente equivalente homologado.
- **Compatibilidade do Ecossistema:** Compatibilidade total dos componentes, drivers e bibliotecas com os sistemas operacionais corporativos Windows 10, Windows 11 (arquiteturas x64 e x86) e macOS e futuras versões suportadas pelo fabricante durante a vigência, bem como com assinadores, plataformas governamentais externas (Gov.br, e-Social) e aplicações adotadas no Poder Judiciário.

1.3.2.3 Requisitos de Capacitação

A licitante vencedora deverá realizar:

- **Orientação Assistida ao Primeiro Uso:** A solução fornecida deve garantir que o processo de ativação inicial seja acompanhado por manuais e orientações técnicas detalhadas direcionadas ao usuário para instalação, configuração de PIN/senha e inicialização do ativo.
- **Disponibilização de Repositório:** Manutenção e disponibilização de drivers atualizados junto à equipe de TI do órgão para homologação na Central de Software, mitigando dúvidas operacionais e suportando a transição gradual dos fluxos tradicionais para o modelo em nuvem.





1.3.2.4 Requisitos de Manutenção

Os requisitos de manutenção devem conter:

- A manutenção dos certificados digitais deverá compreender as ações necessárias para manter os certificados aptos ao uso durante todo o período de validade contratado, abrangendo certificados digitais em nuvem e certificados digitais em mídia física com token USB.
- A licitante vencedora deverá realizar a manutenção corretiva relacionada a falhas técnicas, inconsistências de funcionamento, problemas de ativação, falhas de autenticação, falhas de leitura, indisponibilidade de acesso, incompatibilidades comprovadas ou dificuldades de utilização do certificado digital, quando relacionadas ao serviço prestado.
- Para os certificados digitais em mídia física, a manutenção deverá abranger, quando aplicável, a orientação técnica para uso do token USB, funcionamento dos drivers oficiais, bibliotecas, componentes de integração, leitura do certificado, reconhecimento da mídia criptográfica e utilização em sistemas e assinadores compatíveis.
- Para os certificados digitais em nuvem, a manutenção deverá abranger, quando aplicável, a orientação técnica para ativação, autenticação, acesso, uso do certificado, funcionamento dos mecanismos de autenticação forte, dispositivo autorizado, aplicativo autenticador ou mecanismo equivalente disponibilizado pela solução.
- Deverão estar contempladas nos requisitos de manutenção, no mínimo:
 - Análise e correção de falhas técnicas de funcionamento do certificado digital;
 - Orientação técnica para ativação e utilização do certificado;
 - Apoio à regularização de falhas de acesso, leitura, autenticação ou assinatura digital;





- Verificação de compatibilidade com sistemas, assinadores e aplicações indicadas por este Tribunal.
- A manutenção não deverá gerar ônus financeiro adicional ao PJMT quando relacionada a falhas técnicas, vícios, inconsistências, erros de funcionamento, indisponibilidade ou incompatibilidades decorrentes da prestação dos serviços pelo fornecedor.
- Todos os atendimentos relacionados à manutenção deverão ser obrigatoriamente registrados na ferramenta oficial de gestão de atendimentos do órgão gerenciador, contendo, no mínimo, o diagnóstico realizado, a causa identificada, a providência adotada, as evidências da manutenção executada e a situação final do chamado.

1.3.2.5 Requisitos de Garantia

- Os certificados digitais a serem emitidos deverão possuir validade integral correspondente ao período estimado da contratação de 24 (vinte e quatro) meses, sendo vedada a necessidade de renovações intermediárias durante este intervalo.
- Para os certificados digitais do tipo A3 e-CPF (Cadeia Cert-JUS) em mídia física, a futura contratada deverá fornecer declaração formal de garantia do token USB, com vigência iniciada a partir do recebimento definitivo do lote solicitado, cobrindo integralmente defeitos de fabricação, falhas de funcionamento, vícios técnicos ou incompatibilidades tecnológicas, desde que não decorrentes de mau uso comprovado pelo titular.
- Para os certificados digitais do tipo A3 e-CPF (Cadeia Cert-JUS) em nuvem, a solução escolhida deverá assegurar, durante todo o período de validade do documento digital: a alta disponibilidade da plataforma, a acessibilidade contínua ao certificado, mecanismos de autenticação forte, a custódia rigorosa e segura da chave privada,





a rastreabilidade total das operações e o suporte técnico especializado.

- Os serviços técnicos deverão manter os certificados digitais plenamente operacionais e aptos ao uso, em estrita observância às normativas da ICP-Brasil, às diretrizes da cadeia Cert-JUS, às regras da Autoridade Certificadora responsável e aos requisitos técnicos estabelecidos pelo PJMT.
- Competirá exclusivamente à licitante vencedora, durante a validade do certificado, a prestação de suporte técnico e operacional especializado para a resolução de incidentes relacionados a: emissão, ativação, utilização, leitura, autenticação, assinatura digital, bloqueio, desbloqueio, revogação, substituição ou reemissão dos certificados digitais, sejam eles em nuvem ou em mídia física.
- Constatada qualquer falha técnica, defeito na mídia criptográfica, erro de emissão, incompatibilidade homologada, indisponibilidade da plataforma em nuvem ou incapacidade de uso do certificado por fator atribuível ao fornecedor, este deverá providenciar a imediata correção, substituição, reemissão ou regularização do ativo, sem qualquer ônus financeiro adicional para este Tribunal, respeitados os procedimentos de segurança da informação e normatizações vigentes.

1.3.2.6 Requisitos de Projeto e de Implementação:

Os requisitos de projeto e implementação devem conter:

- Fase de Testes (Prova de Conceito): Após a classificação provisória da licitante em primeiro lugar e antes da adjudicação/homologação definitiva, deverá ser realizada Prova de Conceito, sem ônus para o Tribunal, para verificação de aderência técnica e segurança da solução.





- **Escopo dos Testes:** O fornecedor deverá disponibilizar 6 (seis) certificados digitais de teste (3 em nuvem com MFA e 3 físicos com tokens USB) no prazo de até 5 (cinco) dias úteis após a indicação dos usuários pelo órgão gerenciador, abrindo prazo de até 10 (dez) dias úteis para a execução de testes de compatibilidade nos sistemas institucionais.
- **Estrutura de Atendimento:** Implementação e disponibilização imediata de canais dedicados para suporte (telefone, e-mail ou ticket) após a assinatura do termo de cooperação ou contrato, além da estruturação de dois pontos de atendimento físico obrigatórios nos municípios de Cuiabá/MT e Várzea Grande/MT.

1.3.2.7 Requisitos de Experiência Profissional e Formação de Equipe

- **Alocação de Mão de Obra:** Disponibilização de equipe técnica especializada própria para a execução das atividades de suporte, emissão assistida, validação e manutenção corretiva.
- **Profissionais de Apoio Presencial:** Alocação de recursos humanos qualificados para operar os postos fixos de Cuiabá e Várzea Grande, bem como para a realização das visitas técnicas presenciais nas unidades mapeadas do PJMT, sob demanda e após autorização da fiscalização.

1.3.2.8 Requisitos Temporais

- **Vigência e Ciclo de Vida:** A contratação deverá observar requisitos temporais mínimos com prazos objetivos para assegurar a previsibilidade operacional, o controle da execução e a estabilidade e disponibilidade dos serviços de certificação digital. A vigência estimada para o vínculo será de 24 (vinte e quatro) meses, com início contado a partir da assinatura do instrumento ou da emissão da respectiva ordem de início de serviço. Este prazo foi planejado para acompanhar integralmente o ciclo de vida e a





validade de 24 meses dos certificados emitidos, evitando a necessidade de renovações intermediárias.

- **Disponibilização Imediata de Canais:** Imediatamente após a formalização do vínculo, a licitante vencedora deverá disponibilizar e manter operacionais todos os canais de atendimento e suporte técnico (incluindo telefone, e-mail ou outros meios definidos por este Tribunal) para o registro, triagem e tratamento das demandas institucionais.
- **Fluxo Temporal e Rastreabilidade dos Serviços sob Demanda:** Para todas as atividades executadas sob demanda — tais como emissão, ativação, suporte, substituição, reemissão, bloqueio, revogação ou regularização de ativos —, o fornecedor deverá observar estritamente as seguintes etapas e prazos de controle:
 - a) Registrar o recebimento imediato da solicitação diretamente na ferramenta oficial de gestão de atendimentos do PJMT;
 - b) Executar o fluxo temporal de autorização, emissão de voucher, validação de carta de autorização, agendamento e validação de identidade nos moldes definidos por este Órgão;
 - c) Concluir e dirimir o atendimento dentro das janelas e prazos de Acordo de Nível de Serviço (SLA) e do Instrumento de Medição de Resultados (IMR);
 - d) Manter o respectivo ticket atualizado em tempo real com o andamento da solicitação, diagnósticos realizados, providências adotadas e anexação de evidências físicas da execução.
- **Prazos da Prova de Conceito (PoC):** Na fase de homologação técnica da solução, o cronograma estrito estabelece o prazo de até 5 (cinco) dias úteis para que a empresa classificada em primeiro lugar realize a emissão e a efetiva disponibilização dos certificados de teste aos usuários indicados pelo Tribunal. Ato contínuo, abre-se a janela temporal de até 10 (dez) dias úteis para a execução interna dos testes de compatibilidade técnica, operacional e funcional por parte da equipe técnica do PJMT.





- **Prazos de Logística e Despacho de Hardware:** Para os certificados do tipo A3 em mídia física (Tokens USB), os prazos de preparação, postagem e remessa expressa via SEDEX devem ser formalmente controlados, sendo obrigatório o registro do protocolo de postagem e do código de rastreamento no respectivo ticket em até 8 horas úteis após a providência inicial.
- **Prazos de Atendimento Presencial Extraclasse:** As visitas técnicas presenciais nas unidades e juizados autorizados de Cuiabá e Várzea Grande deverão ser agendadas e integralmente executadas no prazo máximo de até 2 (dois) dias úteis, contados a partir da autorização formal expedida pela fiscalização do órgão, ressalvadas hipóteses excepcionais de reagendamento por indisponibilidade justificada do usuário ou da unidade, devidamente registradas no chamado.
- **Mecanismos de Monitoramento Temporal (IMR):** Todos os prazos de resposta e resolução serão monitorados continuamente pela equipe de fiscalização técnica por meio de indicadores de cumprimento de prazo estabelecidos.

1.3.2.9 Requisitos de Segurança e Privacidade

- **Conformidade Legal e normativa:** A solução proposta deverá observar em todo o seu ciclo de execução as normas, políticas e diretrizes da ICP-Brasil, da cadeia Cert-JUS e as resoluções do Conselho Nacional de Justiça (CNJ). Caso os serviços envolvam a guarda de chaves lógicas, o fornecedor deve dispor de credenciamento ativo como Prestador de Serviço de Confiança (PSC), nos termos do DOC-ICP-17.
- **Tratamento de Dados e LGPD:** As atividades de coleta, validação e tratamento de dados pessoais essenciais para a emissão do e-CPF deverão limitar-se ao mínimo necessário, em estrita observância à Lei Geral de Proteção de Dados Pessoais (LGPD). O





fornecedor deverá assegurar a confidencialidade, integridade e a manutenção de logs e trilhas de auditoria das operações para controle do órgão gerenciador.

- **Segurança Criptográfica e Inviolabilidade:** O acesso às chaves privadas do Tribunal deverá ser mediado por autenticação forte multifator (MFA) e canais criptografados adequados, impossibilitando qualquer tipo de exportação, cópia local ou armazenamento indevido fora dos ambientes criptográficos homologados (mídias físicas ou HSMs com certificação de segurança).
- **Controle de Incidentes e Rastreabilidade:** Em situações de perda, roubo, extravio ou suspeita de uso indevido das credenciais, a solução deve viabilizar ações tempestivas de bloqueio, suspensão ou revogação formal dos certificados. Todas as ocorrências e providências adotadas deverão ser centralizadas e registradas na ferramenta oficial do PJMT, preservando a rastreabilidade integral.
- **Sigilo das informações:** A contratada e os profissionais envolvidos na execução dos serviços deverão preservar o sigilo das informações institucionais, dos dados pessoais e das informações protegidas por restrição legal, mediante assinatura de Termo de Confidencialidade e Sigilo, conforme modelo e condições a serem estabelecidos pelo Tribunal.

1.3.2.10 Requisitos Sociais, Ambientais e Culturais.

Requisitos Ambientais

A emissão de certificados digitais mitiga diretamente os impactos ambientais ao suprimir o uso de papel e insumos de impressão como suporte físico de atos processuais, consolidando a preservação de recursos naturais e eliminando a necessidade de grandes áreas físicas para armazenamento de arquivos.

O fornecedor vencedor deverá adotar mecanismos lógicos e operacionais para promover a tramitação de documentos estritamente em formato eletrônico (como a





geração de vouchers e relatórios parametrizados por sistema), vedando a exigência de impressões físicas de relatórios ou comprovantes de suporte.

As mídias físicas (tokens USB) enviadas deverão ser preferencialmente acondicionadas em embalagens de menor volume possível, fabricadas com materiais recicláveis, reutilizáveis ou biodegradáveis, evitando o uso de plásticos descartáveis no transporte e armazenamento.

Requisitos Sociais

A licitante vencedora deverá cumprir integralmente as obrigações e legislações trabalhistas, previdenciárias e de segurança do trabalho aplicáveis à sua equipe técnica, garantindo a regularidade legal da força de trabalho alocada ao PJMT.

O fornecedor deverá assegurar condições de atendimento acessíveis e canais adaptados às pessoas com deficiência, em estrita conformidade com as diretrizes da Lei Brasileira de Inclusão da Pessoa com Deficiência (Lei nº 13.146/2015), garantindo igualdade de acesso nas rotinas de validação de identidade.

Requisitos Culturais

Considerando a natureza da contratação, não foram identificados impactos culturais relevantes decorrentes da prestação dos serviços, uma vez que o objeto se restringe ao fornecimento e emissão de certificados digitais destinados à autenticação eletrônica dos usuários do Tribunal.

1.3.2.11 Requisitos Legais

No que se refere à execução contratual deverão ser observados os seguintes normativos legais:

- Lei nº 14.133, de 1º de abril de 2021, que institui a Lei de Licitações e Contratos Administrativos;
- Resolução CNJ nº 468, de 15 de julho de 2022 (e alterações introduzidas pela Resolução CNJ nº 616, de 11/03/2025): Dispõe sobre as diretrizes obrigatórias para as contratações de Soluções de Tecnologia da Informação e Comunicação no Poder Judiciário;





- Resolução nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026;
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), bem como os normativos internos do PJMT relacionados à proteção de dados pessoais e à segurança da informação.
- Portaria nº 944/2026 TJMT/PRES, altera dispositivos da Portaria TJMT/PRES n. 987/2019, que regulamenta os procedimentos relativos à certificação digital, à utilização de Token de identidade digital e à tramitação eletrônica de mensagens e documentos oficiais no âmbito do Poder Judiciário do Estado de Mato Grosso
- Normativas da ICP-Brasil e Cadeia Cert-JUS: Resoluções do Comitê Gestor da ICP-Brasil aplicáveis à infraestrutura de chaves públicas nacional e especificidades da cadeia AC-JUS para fins de plena validade e eficácia jurídica dos atos jurisdicionais.

1.3.3 Aderência a padrões e modelos.

1.3.3.1 Modelo Nacional de Interoperabilidade - MNI

O Modelo Nacional de Interoperabilidade (MNI) é o padrão de comunicação estabelecido pelo Conselho Nacional de Justiça (CNJ) para ser utilizado pelos Tribunais, além de outros órgãos, como o Ministério Público e a Advocacia-Geral da União.

O MNI permite que as informações necessárias ao trâmite eletrônico do processo sejam interpretadas em todos os órgãos da Justiça que o utilizam, garantindo a integração segura entre diferentes plataformas processuais.

Nesse contexto, os certificados digitais a serem adquiridos são as ferramentas essenciais que garantem a identidade de quem assina e a segurança dos dados enviados pelos magistrados e servidores do PJMT. Eles asseguram a validade jurídica de todas as comunicações e atos processuais nos sistemas que utilizam o padrão MNI (como o PJe), impedindo que a autoria de uma assinatura digital seja questionada.





1.3.3.2 Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil

Conforme definição apresentada pelo Instituto Nacional de Tecnologia da Informação-ITI, a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil: É uma cadeia hierárquica de confiança, que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão e de instituições.

A conformidade com a ICP-Brasil é totalmente aplicável e mandatória para o presente caso. Todos os certificados digitais de tipo A3 (sejam em mídia física como tokens USB, sejam em nuvem) a serem fornecidos pela CONTRATADA deverão ser emitidos por Autoridade Certificadora (AC) devidamente credenciada e regular perante a ICP-Brasil. A estrita observância a este padrão é o que confere presunção de validade jurídica, integridade e sigilo aos documentos eletrônicos assinados no âmbito deste Poder Judiciário.

1.3.3.3 Modelo de Requisitos Moreq-Jus

Tal modelo, instituído pela Resolução nº 522/2023-CNJ, apresenta os requisitos que os documentos digitais produzidos pelo Judiciário e os sistemas informatizados de gestão documental deverão cumprir no intuito de uniformizar critérios mínimos para garantir a gestão, preservação e segurança de processos e documentos digitais no Judiciário.

A aquisição de certificados digitais guarda relação direta com as premissas de segurança e integridade fixadas pelo Moreq-Jus. A utilização do certificado digital A3 garante que os documentos e processos digitais gerados, armazenados e tramitados no âmbito do PJMT possuam autoria declarada de forma inequívoca e fiquem protegidos contra alterações posteriores à assinatura, cumprindo os requisitos de segurança da informação, cadeia de custódia e preservação de longo prazo exigidos pelo modelo normativo do CNJ.

1.4 Atendimento da Demanda

1.4.1 Portal do Software Público Brasileiro





O Portal do Software Público Brasileiro consolida-se como uma iniciativa que conseguiu criar um ambiente comum para compartilhar soluções de software no setor público, racionalizar a gestão dos recursos de informática, reaproveitar as soluções de software existentes para diminuir custos e atividades redundantes, estabelecer parcerias e ações cooperadas e reforçar a política pública de estimular o uso de software livre.

Contudo, após consulta ao referido portal, verificou-se a inexistência de soluções públicas similares capazes de satisfazer às necessidades desta contratação.

A inviabilidade de aproveitamento de soluções do SPB decorre da natureza do objeto, que não se restringe a um código computacional ou aplicação isolada, mas sim à prestação de serviços de infraestrutura de chaves públicas, validação de identidade e emissão de ativos criptográficos em estrita conformidade com as normas da ICP-Brasil (Cadeia Cert-JUS). Tais serviços exigem credenciamento ativo perante as autoridades competentes, conformidade com o DOC-ICP-17 e custódia tecnológica de alta segurança (módulos criptográficos HSM), requisitos estes que não são supridos por softwares disponibilizados de forma comunitária ou pública.

1.4.2 Soluções de TIC

O objeto da contratação consiste na prestação de serviços de validação e emissão de certificados digitais ICP-Brasil para pessoa física, padrão Cert-JUS A3, nas modalidades em nuvem e com mídia criptográfica (token USB), bem como na realização de visitas técnicas, quando necessárias.

Trata-se de solução padronizada e regulamentada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, sendo os certificados emitidos por Autoridades Certificadoras (AC) credenciadas pelo Instituto Nacional de Tecnologia da Informação (ITI) e operacionalizados por intermédio de Autoridades de Registro (AR), responsáveis pelos procedimentos de validação presencial ou remota da identidade dos titulares.

Atualmente, existem diversas empresas credenciadas na ICP-Brasil aptas a fornecer essa solução, incluindo certificados digitais Cert-JUS nas modalidades em nuvem e com mídia criptográfica, bem como os serviços de validação, emissão, suporte técnico e atendimento presencial, quando necessário. A relação atualizada das





Autoridades Certificadoras e Autoridades de Registro credenciadas pode ser consultada no [Portal de Estrutura da ICP-Brasil \(ITI\)](#)

Para a presente contratação existem as soluções disponíveis no mercado conforme descrito abaixo, vejamos:

Solução 1: Contratação de empresa especializada para emissão e validação de certificados digitais (Modelos em Nuvem e Token USB) credenciada na ICP-Brasil (Cadeia Cert-JUS).

- **Descrição da Solução:** Consiste em terceirizar a infraestrutura de emissão por meio da contratação de um fornecedor especializado e credenciado perante o Instituto Nacional de Tecnologia da Informação (ITI). O parceiro de mercado assume a responsabilidade pelas Autoridades de Registro (AR), validações documentais, fornecimento dos tokens físicos, sustentação da plataforma em nuvem e suporte técnico

Solução 2: Criação de uma Autoridade Certificadora (AC) Privada ou Interna do Poder Judiciário.

- **Descrição da Solução:** Consiste no desenvolvimento e implementação de uma infraestrutura própria e interna de certificação digital gerenciada pelo próprio Tribunal, emitindo identidades lógicas e chaves criptográficas de forma autônoma para consumo exclusivo nos sistemas judiciais internos.

Solução 3: Criação de uma Autoridade Certificadora própria vinculada diretamente à hierarquia da ICP-Brasil.

- **Descrição da Solução:** Envolve a estruturação de uma Autoridade Certificadora institucional (AC-PJMT) formalmente subordinada à cadeia da AC-JUS e homologada junto ao ITI. O Tribunal passaria a ser o custodiante e emissor oficial de certificados e-CPF ICP-Brasil.

1.4.3 Contratações Públicas Similares





O processo de identificação de contratações públicas similares se deu através de acesso ao Portal Nacional de Compras Públicas, Banco de Preços, Radar TCE MT, a partir do parâmetro de pesquisa simplificada pelos termos do objeto a ser contratado.

- **Pregão Eletrônico n. 07/2026 do Tribunal de Justiça do Estado do Rio Grande do Norte**, cujo objeto é Aquisição de vouchers para certificados digitais, visando atender à demanda por serviços de certificação digital.
- **Pregão Eletrônico n. 11/2026 do Ministério Público do Estado de Mato Grosso** cujo objeto é o registro de preços para futura e eventual aquisição de certificados digitais no padrão ICP Brasil e diárias de validação presencial.
- **Pregão Eletrônico n. 18/2026 do Tribunal Regional Eleitoral do Estado de São Paulo**, cujo objeto é o Registro de preços para emissão de certificados digitais dentro das especificações e normas ICP-Brasil, para pessoa física e jurídica, incluindo o fornecimento de dispositivos criptográficos TOKENS USB para armazenamento.

A análise dessas contratações evidencia que o modelo proposto — contemplando emissão e validação de certificados digitais, certificados em nuvem e/ou com mídia criptográfica (token USB), bem como serviços de atendimento presencial quando necessários — encontra ampla utilização na Administração Pública, demonstrando a viabilidade técnica da solução, a existência de fornecedores aptos à sua execução e a aderência da presente contratação às práticas atualmente adotadas por outros órgãos públicos

1.4.4 Soluções similares em outros órgãos

Não foram identificadas soluções tecnicamente distintas ou alternativas disruptivas além daquelas já avaliadas neste Estudo Técnico Preliminar.

1.4.5 Modelos de Aquisição/Prestação do Serviço

Durante a fase de planejamento foram avaliados os modelos de prestação de serviço disponíveis para atendimento da demanda institucional, considerando as características da solução, a evolução tecnológica da certificação digital, as necessidades do Tribunal e as práticas adotadas pela Administração Pública.

Foram analisados os seguintes modelos:





a) Contratação exclusivamente de certificados digitais em mídia criptográfica (token USB): Modelo tradicional, amplamente utilizado pelos órgãos públicos, que demanda fornecimento de dispositivos físicos para armazenamento das chaves criptográficas. Embora apresente elevada segurança e ampla compatibilidade, implica maior custo operacional relacionado à logística de distribuição, substituição e gerenciamento das mídias.

b) Contratação exclusivamente de certificados digitais em nuvem: Modelo que elimina a necessidade de dispositivos físicos, proporcionando maior mobilidade, facilidade de utilização e redução dos custos logísticos. Entretanto, a adoção exclusiva dessa modalidade pode não atender integralmente situações específicas em que ainda seja necessária a utilização de certificados armazenados em mídia criptográfica.

c) Contratação de solução híbrida (certificados em nuvem e em token USB): Modelo que combina as vantagens das duas modalidades, permitindo a utilização de certificados em nuvem como solução preferencial e a disponibilização de certificados em mídia criptográfica para situações específicas, conforme necessidade da Administração.

Após a análise das alternativas, concluiu-se que o modelo híbrido apresenta a melhor relação entre segurança, flexibilidade operacional, estabilidade dos serviços e eficiência administrativa, permitindo a modernização gradual da infraestrutura de certificação digital do Poder Judiciário sem comprometer a compatibilidade com os sistemas atualmente utilizados.

Dessa forma, este Estudo Técnico Preliminar adota como solução recomendada a contratação de empresa especializada para prestação de serviços de certificação digital, contemplando a emissão de certificados digitais em nuvem e em mídia criptográfica (token USB), sob demanda, bem como os serviços correlatos necessários ao gerenciamento do ciclo de vida dos certificados.

1.4.6 Capacidade e alternativas do mercado de TI





O objeto da contratação deste estudo não revelou a existência de alternativas de mercado, além daquelas já expressas e registradas neste estudo.

1.4.7 Contratações correlatas e/ou interdependentes

A presente contratação não possui dependência direta de outras contratações para sua execução, constituindo solução autônoma sob o ponto de vista contratual e operacional.

Todavia, sua utilização integra-se diretamente aos sistemas corporativos e às plataformas tecnológicas do Tribunal que exigem autenticação e assinatura eletrônica para a prática de atos processuais e administrativos, tais como o Processo Judicial Eletrônico (PJe), o PJeOffice e demais aplicações institucionais do Poder Judiciário do Estado de Mato Grosso.

Esclarece-se que os serviços atualmente executados no âmbito do Contrato nº 128/2024 constituem apenas o histórico do parque instalado do órgão, não configurando relação de dependência ou vinculação contratual com o presente certame, o qual se estrutura de forma autônoma e sob nova modelagem tecnológica.

1.5 Análise dos Custos Totais da Demanda

A análise dos Custos Totais de Propriedade busca mensurar os impactos financeiros diretos e indiretos que o Poder Judiciário do Estado de Mato Grosso assumirá ao longo do ciclo de vida de 24 meses da solução de TIC.

A presente análise estabelece a memória de cálculo com base nos parâmetros operacionais obtidos na fase de levantamento de mercado, garantindo a total transparência e a rastreabilidade dos dados orçamentários.

a) Componentes do Ciclo de Vida da Solução Híbrida:

1. **Custos de Aquisição e Emissão (Diretos):** Taxas de validação biométrica perante a ICP-Brasil, emissão das chaves criptográficas na cadeia Cert-JUS (tanto em nuvem quanto físicas) e fornecimento dos tokens USB (hardware).
2. **Custos de Manutenção e Suporte (Garantia Estendida):** O preço unitário obtido em pesquisa absorve a garantia técnica total dos tokens pelo prazo de 24 meses contra defeitos de fabricação ou falhas de *firmware*, além do suporte técnico especializado da Autoridade Certificadora.





3. **Custos de Migração e Treinamento:** Inexistência de custo acessório de treinamento para o Tribunal, visto que a futura contratada deverá fornecer manuais, guias interativos e vídeos de ativação assistida como parte do escopo nativo do serviço. A migração operacional e a emissão de *vouchers* ocorrerão por meio de plataformas corporativas *web* da própria empresa vencedora, sem ônus adicionais de licenciamento.
4. **Custos Logísticos e de Deslocamento:** Custos de frete, postagem e seguro de entrega das mídias físicas nas comarcas (que correrão integralmente por conta do fornecedor), além dos custos de diárias, passagens e alimentação já embutidos no item de Visita Técnica para o interior.

b) Estratégia de Pesquisa de Mercado: Modelagem por Cenários Comparativos

Com o objetivo de identificar a modelagem de contratação mais vantajosa, econômica e eficiente para a Administração, a pesquisa de preços junto ao mercado foi realizada abrangendo duas alternativas de estruturação de itens (Cenários A e B), cujas tabelas analíticas de composição do TCO são apresentadas a seguir:

Cenário A – Solução Integrada (Modelo Combo)

Nesta modelagem, os serviços de emissão e o fornecimento de hardware (Token USB) são contratados de forma conjunta em um único item, mantendo a estrutura tradicional de mercado:

Tabela – Estimativa de TCO - Cenário A (Solução Integrada)

Soluções Identifica das	Especificação do Produto / Serviço	Quantificação do Produto ou Serviço (24 meses)	Valor Unitário Estimado (R\$)	Valor Total Estimado (R\$)
Solução 1 (Cenário A)	Item 1: Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, sem fornecimento de mídia física.	4.000 unidades	R\$ 369,00	R\$ 1.476.000,00
	Item 2: Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com fornecimento integrado de mídia criptográfica (Token USB).	7.000 unidades	R\$ 407,50	R\$ 2.852.500,00





Soluções Identificadas	Especificação do Produto / Serviço	Quantificação do Produto ou Serviço (24 meses)	Valor Unitário Estimado (R\$)	Valor Total Estimado (R\$)
	Item 3: Serviço sob demanda de Visita Técnica para suporte, instalação e validação presencial.	150 visitas	R\$ 275,00	R\$ 41.250,00
Total Cenário A				R\$ 4.369.750,00

Cenário B – Solução Desmembrada (Segregação de Serviço e Hardware)

Nesta modelagem, promove-se a dissociação do "combo" de mídia física, segregando o serviço de emissão biométrica do fornecimento isolado do dispositivo eletrônico (hardware do Token USB), permitindo aferir com precisão os custos específicos de cada insumo:

Tabela Estimativa de TCO - Cenário B (Solução Desmembrada)

Soluções Identificadas	Especificação do Produto / Serviço	Quantificação do Produto ou Serviço (24 meses)	Valor Unitário Estimado (R\$)	Valor Total Estimado (R\$)
Solução 1 (Cenário B)	Item 1: Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, sem fornecimento de mídia física.	4.000 unidades	R\$ 369,00	R\$ 1.476.000,00
	Item 2: Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, destinado a mídias físicas (não inclui o token).	7.000 unidades	R\$ 257,50	R\$ 1.802.500,00
	Item 3: Fornecimento de mídia criptográfica física em formato de Token USB (apenas o hardware/dispositivo).	7.000 unidades	R\$ 200,00	R\$ 1.400.000,00
	Item 4: Serviço sob demanda de Visita Técnica para suporte, instalação e validação presencial.	150 visitas	R\$ 275,00	R\$ 41.250,00
Total				R\$ 4.719.750,00

Análise comparativa dos Cenários A e B

Com base nos valores obtidos na pesquisa de preços, o Cenário A – Solução Integrada apresenta maior vantagem sob a perspectiva do Custo Total de Propriedade (TCO). Considerando o ciclo de vida estimado de 24 (vinte e quatro) meses, o Cenário A





apresenta valor total estimado de R\$ 4.369.750,00, enquanto o Cenário B – Solução Desmembrada totaliza R\$ 4.719.750,00 representando uma diferença estimada de R\$ 350.000,00 em favor da solução integrada.

Embora o Cenário B apresente valores unitários inferiores para os serviços de validação e emissão dos certificados destinados às mídias físicas, essa redução não é suficiente para compensar o custo adicional decorrente da aquisição dos 7.000 tokens USB como itens de hardware individualizados, resultando em valor global superior para a solução desmembrada.

Além da diferença econômica identificada, o desmembramento do fornecimento das mídias físicas acrescentaria maior complexidade à gestão operacional e administrativa da contratação, uma vez que os tokens seriam adquiridos separadamente do serviço de certificação digital. Essa modelagem implicaria procedimentos adicionais relacionados ao recebimento, conferência, armazenamento, distribuição, eventual controle patrimonial, garantia, substituição e descarte das mídias físicas, além da necessidade de compatibilizar a gestão desses dispositivos com os serviços de emissão, ativação e utilização dos certificados.

No Cenário A, por sua vez, o fornecimento dos tokens encontra-se integrado ao serviço de certificação digital, mantendo sob responsabilidade da contratada o fornecimento das mídias e os respectivos serviços de garantia e suporte. Essa configuração reduz a necessidade de controles e procedimentos administrativos adicionais por parte do Tribunal e proporciona maior eficiência na gestão do ciclo de vida dos certificados físicos.

Dessa forma, considerando o menor custo total estimado e a menor complexidade operacional associada à gestão das mídias físicas, o Cenário A – Solução Integrada mostra-se como a alternativa mais adequada para a Administração, devendo ser adotado como referência para a estruturação do Termo de Referência.

A origem dos dados que alimentam as colunas de valores tem como base a média/mediana obtida por meio da pesquisa de preços realizada com as Autoridades Certificadoras do mercado para ambas as modelagens, bem como pelo painel de contratações similares de 2025/2026. Os valores apresentados correspondem ao ciclo de vida estimado de 24 (vinte e quatro) meses da contratação.





c) Justificativa de Não Análise das Soluções 2 e 3

Nota de Exclusão de Soluções Inviáveis:

Esclarece-se que as Soluções 2 e 3 (Criação de Autoridade Certificadora Privada ou própria ICP-Brasil interna) foram classificadas como tecnicamente e administrativamente inviáveis logo na fase preliminar de levantamento de mercado deste ETP.

Por demandarem custos elevados e contínuos de infraestrutura física de TI (salas seguras com auditoria padrão ITI), contratação de softwares proprietários de criptografia e alocação de força de trabalho técnica exclusiva para gerenciar chaves — o que desviaria o PJMT de sua atividade-fim jurisdicional —, tais alternativas foram formalmente descartadas.

Consequentemente, as soluções 2 e 3 não foram objeto de análise detalhada de TCO, concentrando-se os esforços orçamentários, metodológicos e de governança exclusivamente na Solução 1 (Contratação de Terceiros / Modelo Híbrido), única capaz de atender ao interesse público sob o prisma da eficiência e da economicidade.

1.6 Escolha e Justificativa da Solução

1.6.1 Descrição da solução escolhida

A solução escolhida consiste na contratação de empresa especializada para a prestação de serviços sob demanda de validação e emissão de certificados digitais e-CPF (Cadeia Cert-JUS A3) para pessoa física, com validade individual de 24 (vinte e quatro) meses. O modelo de fornecimento é estruturado de forma híbrida, englobando soluções computacionais em nuvem (cloud) e mídias criptográficas físicas, além de suporte presencial assistido.

O escopo da contratação pretendida está consolidado no seguinte quadro estimativo de itens:

Item	Descrição do Objeto	Tipo	Quantidade Estimada	Vigência
1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses para pessoa física, sem fornecimento de mídia criptográfica	Serviço sob demanda	4.000	24 meses





Lote único	2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses para pessoa física, com fornecimento de mídia criptográfica	Serviço sob demanda	7.000	24 meses
	3	Serviço de Visita Técnica para Emissão de Certificados Digitais	Serviço sob demanda	150	24 meses

- **Item 1 – Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3 em Nuvem:** Fornecimento de certificado digital para pessoa física, com armazenamento das chaves criptográficas em solução computacional em nuvem (cloud), dispensando a utilização de mídia criptográfica física, proporcionando maior mobilidade e facilidade de uso pelos usuários.
- **Item 2 – Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3 com Fornecimento de Mídia Criptográfica:** Emissão e validação de chaves criptográficas armazenadas diretamente em dispositivo físico do tipo Token USB novo, fornecido pelo parceiro tecnológico contratado, garantindo a compatibilidade com sistemas legados e atendimento às necessidades operacionais do Tribunal de Justiça.
- **Item 3 – Serviços de Visita Técnica para emissão de Certificados Digitais:** Prestação de visitas técnicas sob demanda para realização de validações presenciais, emissões, renovações e demais atividades relacionadas aos certificados digitais, quando solicitadas pela fiscalização contratual.

Os quantitativos estipulados possuem caráter meramente estimativo e não vinculam o Tribunal à utilização integral. As aquisições ocorrerão de forma fracionada, balizadas pela demanda real de magistrados e servidores, mediante os instrumentos formais de controle e autorização prévia de vouchers instituídos pela fiscalização do órgão.

1.6.2 Motivação da Escolha

1.6.2.1 Contexto e Justificativa

A escolha da solução fundamenta-se na necessidade de prover ao Poder Judiciário do Estado de Mato Grosso uma infraestrutura de identidade digital robusta,





móvel e altamente disponível, capaz de suportar o volume crescente de processos eletrônicos e garantir a validade jurídica dos atos jurisdicionais.

A eventual ausência ou deficiência no fornecimento de certificados digitais e-CPF A3 provocaria impactos diretos e imediatos nos serviços prestados aos usuários e à sociedade, tais como:

- Para Magistrados e Assessores: Impossibilidade técnica de assinar eletronicamente minutas, decisões, despachos e sentenças nos sistemas processuais (PJe), paralisando o fluxo de julgamentos no 1º e 2º Grau.
- Para Audiências e Atendimento Telepresencial: Inviabilidade de autenticação e validação de atos praticados durante audiências virtuais e sessões de julgamento, gerando o risco de cancelamento de pautas e atrasos nas deliberações.
- Para Servidores e Unidades Administrativas: Bloqueio de acesso a sistemas governamentais obrigatórios (como e-Social e Gov.br) e inviabilização da tramitação de processos administrativos internos, gerando retrabalho e gargalos operacionais.
- Para a Sociedade e o Jurisdicionado: Risco de morosidade na expedição de alvarás, mandados e liminares urgentes, comprometendo a celeridade e a efetividade da tutela jurisdicional prestada ao cidadão.

Nesse contexto, a escolha pelo modelo híbrido (nuvem + token físico) maximiza os benefícios para a instituição: enquanto a certificação em nuvem confere agilidade, facilidade de gestão de senhas e autonomia de uso em múltiplos dispositivos, a manutenção de mídias físicas assegura contingência e compatibilidade com sistemas legados, eliminando riscos de descontinuidade operacional.

Justificativa para não adoção da Solução 2

A alternativa consistente na criação de uma Autoridade Certificadora (AC) própria para utilização exclusiva pelo Tribunal foi considerada inviável. Sua implantação demandaria investimentos elevados em infraestrutura criptográfica, aquisição de Módulo de Segurança em Hardware (HSM), implementação de ambiente altamente seguro, formação de equipe técnica especializada, desenvolvimento de processos próprios de certificação e manutenção permanente da infraestrutura.

Além do elevado custo de implantação e operação, essa alternativa não atenderia ao objetivo institucional de emissão de certificados digitais ICP-Brasil com reconhecimento nacional, limitando sua utilização aos sistemas internos do Tribunal.





Dessa forma, concluiu-se que a solução apresenta baixa relação custo-benefício para atendimento da demanda.

Justificativa para não adoção da Solução 3

Também foi analisada a possibilidade de estruturação de uma Autoridade Certificadora própria vinculada à cadeia da ICP-Brasil. Entretanto, essa alternativa exigiria credenciamento junto ao Instituto Nacional de Tecnologia da Informação (ITI), atendimento a rigorosos requisitos técnicos, operacionais e de segurança, manutenção permanente da infraestrutura de certificação, realização de auditorias periódicas e constituição de estrutura administrativa especializada.

Além da elevada complexidade técnica e regulatória, o modelo acarretaria significativo aumento dos custos de implantação e operação, incompatível com as necessidades institucionais do Tribunal. Dessa forma, concluiu-se que essa alternativa não apresenta vantagem técnica ou econômica em relação à contratação de empresa especializada já credenciada perante a ICP-Brasil.

Justificativa da Solução Escolhida

Dentre as alternativas avaliadas, a contratação de empresa especializada credenciada na ICP-Brasil mostrou-se a solução mais vantajosa sob os aspectos técnico, operacional e econômico. A utilização de fornecedor especializado permite ao Tribunal usufruir de infraestrutura de certificação consolidada, profissionais especializados, conformidade permanente com os requisitos estabelecidos pela ICP-Brasil e atualização contínua da solução tecnológica, sem necessidade de investimentos próprios em infraestrutura de certificação.

Além disso, a adoção de modelo híbrido, contemplando certificados digitais em nuvem e em mídia criptográfica (token USB), possibilita incorporar a evolução tecnológica da certificação digital, ampliar a mobilidade dos usuários e reduzir gradativamente a dependência de dispositivos físicos, preservando a compatibilidade com os sistemas atualmente utilizados pelo Tribunal.





A solução também permite maior eficiência operacional, redução dos custos indiretos relacionados à logística de distribuição de mídias criptográficas, melhoria da experiência do usuário e fortalecimento da segurança da informação.

Considerando os aspectos técnicos, econômicos, operacionais e de governança avaliados durante a fase de planejamento, conclui-se que essa alternativa apresenta a melhor relação custo-benefício para atendimento das necessidades institucionais do Tribunal de Justiça do Estado de Mato Grosso.

Aspectos Observados na Execução Contratual

Durante a execução do Contrato nº 128/2024 foram identificadas oportunidades de melhoria relacionadas à logística de distribuição, aos mecanismos de atendimento, ao gerenciamento das solicitações, ao acompanhamento dos indicadores de desempenho e à modernização da solução tecnológica, aspectos que foram considerados na definição dos requisitos da nova contratação:

Aspecto observado	Impacto Diagnosticado	Tratamento na nova contratação
Dependência exclusiva de token físico	Elevada carga de logística reversa e maior probabilidade de falhas de hardware.	Introdução do certificado em nuvem
Exigência rígida de atendimento presencial	Custos acessórios com deslocamentos intermunicipais e pagamento de diárias.	Validação remota via videoconferência quando aplicável.
Gestão de chamados	Baixa rastreabilidade de suporte e dificuldade de auditoria de interações.	Integração obrigatória com a ferramenta oficial de gestão de atendimentos do órgão.
Distribuição de mídias	Atrasos na entrega de tokens e desabastecimento local de hardware.	Requisitos específicos de logística expressa com prazos estritos de rastreamento.
Controle contratual	Dificuldade de fiscalização e monitoramento da qualidade do serviço.	Aprimoramento dos indicadores de desempenho por meio do Instrumento de Medição de Resultados (IMR).





1.6.3 Benefícios esperados

A contratação proporcionará benefícios institucionais diretamente relacionados ao fortalecimento da transformação digital, à garantia de regularidade do fornecimento e celeridade dos serviços jurisdicionais e ao aprimoramento da governança da identidade digital no âmbito do Tribunal de Justiça do Estado de Mato Grosso.

Destacam-se, como principais benefícios resultantes da solução:

- Fortalecimento da segurança da informação e da identidade digital institucional;
- Modernização da infraestrutura de certificação digital mediante a introdução de certificados em nuvem;
- Aumento da maturidade tecnológica da solução de certificação digital;
- Fortalecimento da governança sobre o ciclo de vida dos certificados digitais;
- Garantia de ininterrupção na assinatura de sentenças e minutas no PJe durante todo o fluxo do 1º e 2º Graus
- Maior aderência às diretrizes da ICP-Brasil, da cadeia Cert-JUS e às políticas de transformação digital do Poder Judiciário;
- Incremento da eficiência administrativa e da qualidade dos serviços prestados aos usuários internos e, indiretamente, aos jurisdicionados.

1.6.4 Resultados Esperados

Com a implantação da solução, espera-se alcançar os seguintes resultados operacionais:

- Disponibilização da modalidade de certificados digitais em nuvem aos usuários autorizados;
- Redução da dependência de mídias criptográficas para emissão e utilização dos certificados;
- Redução da necessidade de deslocamentos para emissão e renovação de certificados, quando aplicável;





- Melhoria da disponibilidade e da sustentação dos serviços de certificação digital;
- Aperfeiçoamento do controle e da rastreabilidade do ciclo de vida dos certificados;
- Melhoria da qualidade do atendimento e do suporte aos usuários;
- Otimização dos processos de emissão, renovação, revogação e substituição de certificados;
- Redução dos custos indiretos relacionados à logística de distribuição de mídias criptográficas;
- Maior eficiência da fiscalização contratual, mediante mecanismos de acompanhamento da execução dos serviços.

1.6.5 Relação entre a Demanda Prevista e a Contratada

A estimativa dos quantitativos da presente contratação foi elaborada com base em critérios técnicos e metodológicos, considerando o histórico de utilização dos serviços no Poder Judiciário do Estado de Mato Grosso (PJMT), o universo de usuários elegíveis, a projeção de novas demandas e a estratégia institucional de modernização e transição tecnológica da certificação digital.

Para a definição da quantidade estimada de 11.000 certificados digitais (sendo 7.000 em mídia criptográfica e 4.000 em nuvem) e 150 visitas técnicas, foram considerados os parâmetros e a metodologia a seguir:

a) Dimensionamento do Público Potencial e Panorama Atual

Foram mapeados os usuários que, em razão de suas atribuições institucionais, necessitam obrigatoriamente de certificado digital ICP-Brasil para a assinatura eletrônica de atos processuais e administrativos, autenticação no PJe e demais sistemas internos ou governamentais externos (como e-Social e Gov.br). O quadro funcional e a distribuição de certificados ativos estão estruturados da seguinte forma:

- Desembargadores: 39
- Magistrados: 309
- Servidores: 5.380
- Total de usuários: 5.728
- Total de certificados ativos atualmente: 5.065.





Os certificados ativos representam aproximadamente 88,34% do quadro funcional, evidenciando que a certificação digital é ferramenta institucional amplamente utilizada e consolidada na rotina do Poder Judiciário.

b) Histórico de utilização e Cronograma de Renovações:

A estimativa levou em consideração o histórico de consumo efetivamente verificado nas contratações anteriores e na contratação vigente (Contrato nº 128/2024), mapeando os respectivos ciclos de vencimento e as renovações obrigatórias previstas para o período de vigência da futura contratação:

Origem	Emissões	Vencimento
Rio Madeira	1.347	2026
Rio Madeira	235	2027
Soluti (2024)	245	2027
Soluti (2025)	2.232	2028
Soluti (2026 até 07/07)	1.006	2029
Total	5.065	-

Do total de 5.065 certificados, há uma necessidade conhecida e consolidada de renovação de 4.059 certificados até dezembro de 2028. Os 1.006 certificados restantes possuem vencimento previsto para 2029, conforme cronograma abaixo:

- 2026: 1.347 certificados
- 2027: 480 certificados
- 2028: 2.232 certificados
- 2029: 1.006 certificados

c) Variáveis que Impactam a Demanda e Metodologia de Cálculo

Para garantir a disponibilidade do fornecimento e o adequado planejamento da Ata de Registro de Preços (ARP), a modelagem de estoque e projeção futura considerou variáveis previsíveis e imprevisíveis divididas em quatro grandes eixos:

1. Crescimento Institucional: Expansão do quadro funcional, novas nomeações e ingresso de magistrados e servidores.





2. Emissões Extraordinárias: Substituições e re emissões decorrentes de eventos cotidianos de suporte, tais como perda, roubo, extravio, dano físico, bloqueios de senha ou defeitos no dispositivo.
3. Necessidades Operacionais: Atendimento a usuários que necessitam de mais de um certificado, demandas específicas de unidades e novas necessidades da Administração.
4. Margem de Planejamento da ARP: Margem técnica indispensável para absorver a flutuação de pessoal, evitar novas licitações prematuras e mitigar demandas futuras imprevistas ao longo dos 24 meses de vigência.

A consolidação desses fatores resultou na seguinte metodologia de cálculo para a composição do limite da Ata:

Componente	Fundamentação	Quantidade
Parque atual/demanda de renovação	Certificados ativos que demandarão renovações durante a vigência da ARP.	5.065
Crescimento institucional	Expansão do quadro funcional e novas nomeações.	800
Emissões extraordinárias	Perdas, danos, bloqueios, defeitos e substituições.	300
Necessidades operacionais	Casos específicos de utilização e múltiplos certificados.	300
Margem de planejamento da ARP	Atendimento da demanda potencial e sustentação dos serviços.	535
Subtotal- certificados em mídia física		7.000

d) Estratégia de Evolução Tecnológica (Migração para Nuvem)

A contratação contempla, pela primeira vez, a disponibilização de certificados digitais em nuvem no âmbito do PJMT, com o objetivo de promover a transição gradual, segura e planejada do modelo tradicional baseado em mídias físicas para uma solução mais moderna, flexível e aderente às atuais necessidades de mobilidade dos usuários.





- Para a modalidade em nuvem, foi estimada a contratação de 4.000 certificados, quantitativo definido como limite máximo para os 24 (vinte e quatro) meses de vigência, sem implicar obrigação de consumo integral pela Administração. O quantitativo foi estabelecido considerando o universo de usuários potencialmente elegíveis, compreendendo magistrados e servidores que utilizam ou necessitam utilizar certificados digitais para o desempenho de suas atividades institucionais, especialmente aqueles que apresentam maior necessidade de mobilidade, como usuários que exerçam funções de coordenação e gestão, servidores em regime de teletrabalho, servidores que desempenhem atividades externas, Oficiais de Justiça e demais usuários que necessitem realizar assinaturas eletrônicas a partir de diferentes localidades e dispositivos autorizados e a estratégia de adoção gradual da nova modalidade, especialmente em razão de sua introdução inédita no PJMT e da necessidade de avaliar sua aderência às necessidades institucionais.

Em um primeiro momento, a adoção da modalidade em nuvem será direcionada aos magistrados e à realização dos testes necessários à validação da solução em ambiente institucional. Essa etapa permitirá avaliar a facilidade de utilização, a compatibilidade com os sistemas corporativos e judiciais, o desempenho, a segurança e a estabilidade da solução, bem como identificar eventuais ajustes necessários antes de sua ampliação.

Após a validação institucional e observados os níveis de eficiência atingidos, a modalidade em nuvem será gradativamente estendida aos demais perfis de usuários conforme vencimentos e novos pedidos, garantindo mobilidade total para a prática de atos processuais a partir de múltiplos dispositivos autorizados.

A ampliação da modalidade em nuvem observará as necessidades institucionais, a aderência da solução e a disponibilidade do quantitativo contratado, mantendo-se a modalidade em mídia física para usuários ou situações em que a solução em nuvem não seja tecnicamente adequada. Com a consolidação da nova modalidade, espera-se ampliar a mobilidade dos usuários e reduzir gradativamente a dependência de mídias criptográficas físicas, bem como os custos e esforços operacionais associados à aquisição, distribuição, substituição e logística de tokens.





- Manutenção de Mídias Físicas (Item 2 - Token USB): O quantitativo de 7.000 unidades assegura o suporte ininterrupto e a estabilidade operacional para os usuários que ainda dependem do modelo físico por razões de compatibilidade com sistemas específicos, preferências de usabilidade de magistrados ou contingências operacionais em que a solução em nuvem não se mostre adequada.

e) Visitas técnicas presenciais

A estimativa de 150 visitas técnicas presenciais foi definida considerando a necessidade de atendimento às unidades do Poder Judiciário localizadas nos municípios de Cuiabá/MT e Várzea Grande/MT, mediante prévia autorização da fiscalização contratual, para atividades de emissão, validação, ativação e suporte aos certificados digitais.

f) Conclusão da estimativa

Com base nos parâmetros apresentados, conclui-se que a estimativa de 11.000 certificados digitais, distribuídos entre 4.000 certificados digitais Cert-JUS A3 em nuvem e 7.000 certificados digitais Cert-JUS A3 com fornecimento de mídia criptográfica (token USB), bem como de 150 visitas técnicas presenciais, é suficiente para atender às necessidades do Poder Judiciário do Estado de Mato Grosso durante os 24 meses de vigência contratual.

Os quantitativos estimados são compatíveis com o universo de usuários elegíveis, o histórico de utilização da solução, a previsão de renovações e substituições, a adoção gradual da certificação em nuvem e as demais demandas institucionais identificadas.

Ressalta-se que os quantitativos possuem natureza estimativa e serão executados sob demanda, não gerando obrigação de consumo integral pela Administração, constituindo apenas o limite máximo estimado para atendimento da demanda ao longo da vigência e adequado planejamento da contratação.

	Item	Descrição do Objeto	Tipo	Quantidade Estimada	Vigência
--	------	---------------------	------	---------------------	----------





Lote Único	1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses para pessoa física, sem fornecimento de mídia criptográfica	Serviço sob demanda	4.000	24 meses
	2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses para pessoa física, com fornecimento de mídia criptográfica	Serviço sob demanda	7.000	24 meses
	3	Serviço de Visita Técnica para Emissão de Certificados Digitais	Serviço sob demanda	150	24 meses

1.6.6 Da intenção de Registro de Preço

Considerando as características da contratação, conclui-se que a adoção do Sistema de Registro de Preços (SRP) mostra-se adequada e vantajosa para atender às necessidades do Tribunal de Justiça do Estado de Mato Grosso.

A demanda por serviços de validação e emissão de certificados digitais possui natureza variável, uma vez que depende de fatores como nomeações de magistrados e servidores, renovações, substituições, revogações, perdas, comprometimento de certificados e demais necessidades institucionais que surgem ao longo da vigência contratual. Assim, embora seja possível estimar o quantitativo global da contratação, não é possível definir previamente o momento exato em que cada serviço será demandado pela Administração.

Além disso, a solução escolhida contempla duas modalidades de certificação digital — certificados em nuvem e certificados em mídia criptográfica (token USB). Considerando que a implantação da certificação em nuvem ocorrerá de forma gradual, coexistindo com o modelo tradicional durante o período de transição tecnológica, a utilização do Sistema de Registro de Preços permitirá que a Administração ajuste o consumo de cada modalidade conforme a evolução das necessidades institucionais, evitando aquisições superiores às efetivamente necessárias e conferindo maior flexibilidade à gestão contratual.

A adoção do SRP também possibilita que as contratações ocorram de forma parcelada, conforme a efetiva necessidade da Administração, contribuindo para a otimização dos recursos públicos, o melhor planejamento orçamentário e financeiro





e a regularidade ininterrupta na prestação dos serviços, sem a necessidade de contratação imediata da totalidade dos quantitativos estimados.

A utilização do Sistema de Registro de Preços encontra respaldo no inciso V do art. 3º do Decreto nº 11.462, de 31 de março de 2023, que prevê sua adoção quando, em razão da natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Após a emissão da nota de empenho e da correspondente solicitação de fornecimento, será celebrado o instrumento contratual, por se tratar de prestação de serviços continuados, contendo as obrigações das partes, as condições de execução, os níveis de serviço e os demais requisitos estabelecidos no Termo de Referência.

Dessa forma, considerando tratar-se de serviços comuns de Tecnologia da Informação e Comunicação, conclui-se que a realização de Pregão Eletrônico, com adoção do Sistema de Registro de Preços, constitui a estratégia de contratação mais adequada para atender às necessidades do Tribunal de Justiça do Estado de Mato Grosso.

A Ata de Registro de Preços terá vigência de 1 (um) ano, podendo ser prorrogada, por igual período, desde que comprovado o preço vantajoso, nos termos do art. 84 da Lei n. 14.133/2021.

1.6.7 Estimativa de custo total da solução escolhida

Os valores unitários e total referentes a toda solução constam da tabela abaixo.





Registro de Preços para Certificados Digitais Cert-JUS A3 - 24 meses

Registro de Preços para Certificados Digitais Cert-JUS A3 - 24 meses														
LOTE	Item	Descrição	Tipo	Qtd	PREÇOS PRIVADOS			PREÇO PÚBLICO		Valor Unitário Média	Valor Unitário Mediana	Valor Total Média	Valor Total Mediana	
					Xdigital Brasil	AR RP Certificação	Certisign	Valid	Contrato n. 128/2024 TJMT					Contrato n. 13/2024 MTI
Lote Único	1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses (e-CPF) para pessoa física (e-CPF), sem fornecimento de mídia criptográfica.	Serviço	4000	R\$ 530,00	R\$ 660,00	R\$ 183,99	R\$ 208,00	-	-	R\$ 395,50	R\$ 369,00	R\$ 1.582.000,00	R\$ 1.476.000,00
	2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses (e-CPF) para pessoa física com o fornecimento do token.	Serviço	7000	R\$ 420,00	R\$ 790,00	R\$ 282,99	R\$ 395,00	-	-	R\$ 472,00	R\$ 407,50	R\$ 3.304.000,00	R\$ 2.852.500,00
	3	Serviço de Visita Técnica para Emissão de Certificados Digitais	Serviço	150	R\$ 450,00	R\$ 300,00	R\$ 1.859,00	R\$ 250,00	R\$ 20,00	R\$ 37,00	R\$ 486,00	R\$ 275,00	R\$ 72.900,00	R\$ 41.250,00
	TOTAL										R\$ 1.353,50	R\$ 1.051,50	R\$ 4.958.900,00	R\$ 4.369.750,00
TOTAL DA ATA DE REGISTRO DE PREÇOS PARA 24 MESES													R\$ 4.369.750,00	

O valor total da contratação corresponde ao montante de R\$ 4.369.750,00(quatro milhões trezentos e sessenta e nove mil setecentos e cinquenta reais), para o período de 24 (vinte e quatro) meses.





1.7 Declaração de viabilidade da contratação

Com base nos estudos realizados, nas análises técnicas e econômicas apresentadas neste Estudo Técnico Preliminar e nas necessidades identificadas pela área demandante, conclui-se que a presente contratação é viável, atendendo ao interesse público e aos objetivos institucionais do Tribunal de Justiça do Estado de Mato Grosso.

A solução proposta encontra-se alinhada ao planejamento institucional e às diretrizes de Tecnologia da Informação e Comunicação do Tribunal, observando os princípios da eficiência, da economicidade, da continuidade dos serviços públicos, da segurança da informação e da transformação digital.

A avaliação das alternativas disponíveis demonstrou que a contratação de empresa especializada para prestação de serviços de validação e emissão de certificados digitais Cert-JUS A3 para pessoa física, contemplando certificados em nuvem e em mídia criptográfica (token USB), representa a alternativa mais vantajosa sob os aspectos técnico, operacional e econômico. A solução permitirá a modernização gradual da infraestrutura de certificação digital do Tribunal, assegurando a estabilidade ininterrupta das atividades jurisdicionais e ampliando a disponibilidade de mecanismos seguros e móveis de autenticação e assinatura eletrônica.

Além disso, verificou-se que a solução apresenta ampla disponibilidade no mercado, possui fornecedores tecnicamente qualificados para sua execução e atende aos requisitos estabelecidos pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), pela cadeia Cert-JUS e pelos demais normativos aplicáveis.

A contratação contribuirá, ainda, para o fortalecimento da transformação digital do Poder Judiciário, ampliando a utilização de tecnologias mais modernas de certificação digital, promovendo maior mobilidade aos usuários, aprimorando a segurança da informação e proporcionando maior eficiência na gestão do ciclo de vida dos certificados digitais.

Diante do exposto, a Equipe de Planejamento da Contratação manifesta-se favoravelmente ao prosseguimento da contratação, por entender que a solução proposta é tecnicamente adequada, economicamente vantajosa e suficiente para atender às necessidades institucionais do Tribunal de Justiça do Estado de Mato Grosso, observadas as condições e especificações que serão estabelecidas no Termo de Referência.





2. SUSTENTAÇÃO DO CONTRATO

2.1 Adequação do ambiente

Infraestrutura tecnológica: Não se prevê a necessidade de adequação estrutural ou aquisição de infraestrutura tecnológica adicional por parte deste Tribunal para a utilização e a implantação dos certificados digitais mapeados nesta solução.

A solução a ser adquirida deverá ser nativamente compatível com o ambiente tecnológico atualmente utilizado no PJMT, incluindo de forma obrigatória os sistemas judiciais e administrativos, assinadores digitais, navegadores de internet, sistemas operacionais homologados, PJeOffice, aplicações corporativas e demais plataformas institucionais que demandem certificação digital.

A coexistência e a adoção dos modelos de certificados digitais em nuvem e em mídia física deverão ocorrer sem impacto relevante à infraestrutura técnica do órgão, competindo ao fornecedor vencedor a disponibilização e atualização de todos os componentes, drivers, bibliotecas, orientações técnicas e mecanismos de integração necessários ao pleno funcionamento da solução.

Eventuais necessidades de instalação, configuração ou atualização de componentes lógicos — tais como drivers, bibliotecas PKCS#11, integração MSCAPI/CSP, aplicativos de autenticação multifator ou módulos de assinatura — deverão ser executadas ou orientadas tecnicamente pelo fornecedor, sem gerar demandas de alteração estrutural no ambiente de rede do Poder Judiciário.

Como mecanismo de salvaguarda e mitigação de riscos, a solução escolhida será submetida a uma fase eliminatória de testes e homologação técnica de compatibilidade frente aos sistemas locais e, quando aplicável, com as plataformas e assinadores geridos pelo Conselho Nacional de Justiça (CNJ).

Ajustes pontuais de parametrização, instalação de componentes locais ou rotinas de orientação de uso não serão considerados adequação de infraestrutura, mas premissas operacionais obrigatórias de implantação e suporte da solução, devendo estar integralmente contempladas no escopo do fornecedor, sem qualquer ônus financeiro adicional para a instituição.





As ações de suporte voltadas à transição do modelo de mídias físicas para a tecnologia em nuvem (orientações sobre ativação, autenticação forte e autorização de múltiplos dispositivos) serão tratadas como plano de aculturação e gestão da mudança, sem caracterizar necessidade de readequação tecnológica estrutural das redes do PJMT.

Infraestrutura elétrica: As unidades já possuem toda a infraestrutura elétrica para o uso pleno da solução.

Logística de implantação/execução: Para os certificados digitais do tipo A3 com fornecimento de mídia criptográfica física, conforme previsto no Item 2 – Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3 para Pessoa Física com fornecimento de mídia criptográfica, será necessária a adoção de logística específica para fornecimento, envio, acompanhamento, entrega e eventual substituição dos tokens USB.

O fornecedor será integralmente responsável pela logística de fornecimento e distribuição dos tokens físicos, incluindo separação, embalagem, postagem, envio, rastreamento, acompanhamento da entrega e regularização de eventuais falhas relacionadas à remessa dos dispositivos, sem ônus financeiro adicional a este Tribunal.

Espaço físico e mobiliário: As unidades já possuem espaço físico e mobiliário para o uso pleno da solução.

2.2 Dos Recursos Materiais e Humanos

- **Recursos Materiais:** Por parte do fornecedor vencedor: Disponibilização e custeio total dos certificados digitais em si, fornecimento de mídias criptográficas físicas novas (tokens USB), disponibilização de drivers oficiais atualizados, bibliotecas técnicas, APIs e componentes lógicos de integração. Também engloba o fornecimento de manuais didáticos, mecanismos de autenticação forte (MFA/biometria), infraestrutura de certificação em nuvem, HSMs certificados, além de todos os recursos de embalagem, postagem (SEDEX) e transporte para envio, substituição ou regularização dos dispositivos.

Por parte deste Tribunal (PJMT): Não se prevê a necessidade de aquisição de infraestrutura tecnológica, servidores de rede, links ou materiais





adicionais, visto que a solução proposta utilizará o ecossistema tecnológico e as estações de trabalho já existentes no órgão.

Premissa de Custeio: Todos os insumos lógicos e físicos detalhados devem estar integralmente embutidos nos custos propostos, sendo vedada qualquer cobrança financeira adicional por insumos inerentes ao perfeito funcionamento da solução de certificação digital.

- **Recursos Humanos:** Por parte do fornecedor vencedor: Alocação de mão de obra especializada para a execução contínua de serviços de emissão, validação, ativação, suporte técnico especializado, manutenção corretiva, substituição, reemissão, bloqueio e revogação de certificados digitais (físicos e em nuvem). A equipe deverá ser apta a realizar atendimentos remotos, suporte presencial (quando autorizado), prestar apoio técnico durante a fase de Prova de Conceito e realizar o registro mandatório das interações na ferramenta oficial de chamados.

Por parte deste Tribunal (PJMT): Dedicção de servidores para atuar na gestão e fiscalização contratual. Esse esforço compreende a indicação de usuários autorizados, controle e emissão de vouchers e cartas de autorização, monitoramento de tickets, homologação técnica da solução, condução dos testes de compatibilidade e suporte na comunicação interna a magistrados e servidores.

2.3 Continuidade do Fornecimento

A continuidade da prestação dos serviços de certificação digital é indispensável ao funcionamento das atividades jurisdicionais e administrativas do Poder Judiciário do Estado de Mato Grosso, uma vez que os certificados digitais são utilizados para autenticação de usuários, assinatura eletrônica de documentos, acesso aos sistemas corporativos e utilização de serviços disponibilizados por outros órgãos da Administração Pública.

Nesse contexto, a presente contratação foi estruturada de forma a assegurar a continuidade do fornecimento durante todo o período contratual, evitando interrupções





que possam comprometer a prestação dos serviços institucionais, com base nas seguintes premissas:

- Validade Residual dos Ativos: Os certificados emitidos sob a égide do contrato vigente (Contrato nº 128/2024) permanecerão ativos e operacionais até o término de suas respectivas validades individuais, eliminando a necessidade de revogações em massa ou substituições antecipadas.
- Mitigação por Demanda Fracionada: O faturamento dos serviços ocorrerá de forma mensal, por consumo efetivo baseado nos serviços já realizados, garantindo que a transição entre os instrumentos não acarrete sobreposição ou duplicidade de custos fixos para o erário.

A introdução da modalidade de certificados digitais em nuvem ocorrerá de forma gradual, coexistindo com a utilização de certificados em mídia criptográfica durante o período de adaptação tecnológica. Essa estratégia reduz riscos operacionais, preserva a compatibilidade com os sistemas atualmente utilizados pelo Tribunal e assegura que a migração para a nova tecnologia ocorra sem prejuízo à continuidade das atividades institucionais.

Além disso, a utilização do Sistema de Registro de Preços possibilitará a emissão dos certificados conforme a necessidade da Administração ao longo da vigência da Ata, contribuindo para a manutenção da disponibilidade dos serviços e para o adequado atendimento das demandas institucionais.

2.4 Transição Contratual e encerramento do contrato

A transição entre o contrato vigente e a futura contratação deverá ocorrer de forma planejada e coordenada, com o objetivo de assegurar a continuidade da prestação dos serviços de certificação digital e evitar impactos às atividades jurisdicionais e administrativas do Tribunal de Justiça do Estado de Mato Grosso.

Durante a vigência contratual, a Administração deverá acompanhar continuamente a execução dos serviços e a evolução tecnológica das soluções de certificação digital disponíveis no mercado, de forma a subsidiar futuras contratações e





verificar se a solução adotada permanece tecnicamente adequada, segura e economicamente vantajosa para o Tribunal.

Com antecedência suficiente ao término da vigência contratual, deverão ser realizados os estudos necessários para definição da estratégia de continuidade da prestação dos serviços, contemplando, conforme o caso:

- A análise da vantajosidade de eventual prorrogação contratual, quando legalmente cabível;
- O planejamento tempestivo de nova contratação, de forma que a futura solução esteja disponível antes do encerramento do contrato vigente, evitando qualquer solução de continuidade na prestação dos serviços.

Na hipótese de substituição da contratada, a transição deverá ser conduzida de forma planejada, garantindo, no mínimo:

- A continuidade da emissão, renovação, revogação e demais serviços relacionados ao ciclo de vida dos certificados digitais;
- A manutenção do atendimento aos usuários durante todo o período de transição;
- A preservação da compatibilidade da solução com os sistemas corporativos utilizados pelo tribunal;
- A disponibilização das informações necessárias à continuidade da prestação dos serviços, observadas as normas de segurança da informação e proteção de dados;
- A adoção das medidas necessárias para evitar impactos às atividades institucionais durante a substituição contratual.

Considerando que a presente contratação introduzirá a modalidade de certificados digitais em nuvem, a transição deverá contemplar a coexistência das modalidades em nuvem e em mídia criptográfica (token USB), quando necessário, permitindo que a migração tecnológica ocorra de forma gradual, segura e sem prejuízo à continuidade dos serviços prestados pelo Tribunal.

Ao encerramento da execução contratual, a contratada deverá cumprir integralmente as obrigações previstas no instrumento contratual, inclusive aquelas relacionadas à conclusão dos serviços em andamento, à disponibilização das informações necessárias à continuidade da solução e às demais providências indispensáveis para assegurar a adequada transição para eventual nova contratação, conforme detalhamento a ser estabelecido no Termo de Referência.





A solução deverá, ainda, ser estruturada de forma a evitar dependência tecnológica da contratada, assegurando que eventual substituição do fornecedor possa ocorrer sem comprometimento da continuidade dos serviços, da integridade das informações e da utilização dos certificados digitais emitidos durante a execução contratual.

2.5 Estratégia de Independência Tecnológica

A estratégia adotada para assegurar a independência tecnológica deste Tribunal em relação ao fornecedor baseia-se na ampla interoperabilidade, na reversibilidade dos dados e no estrito alinhamento com padrões abertos de mercado, conforme diretrizes abaixo:

- Utilização de certificados digitais emitidos em conformidade com as normas da ICP-Brasil e da cadeia Cert-JUS, garantindo que a arquitetura criptográfica siga padrões públicos e auditáveis;
- Compatibilidade da solução com os sistemas corporativos e aplicações utilizados pelo Tribunal;
- Adoção de tecnologias amplamente difundidas no mercado, assegurando interoperabilidade e sustentação dos serviços;
- Inexistência de mecanismos que imponham dependência tecnológica da Administração em relação ao fornecedor;
- Possibilidade de substituição da contratada ao término da vigência contratual, sem risco de descontinuidade ou prejuízo à ininterrupção dos serviços jurisdicionais.

A estratégia de contratação também observará que a relação jurídica entre o titular do certificado digital e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) permaneça preservada durante toda a vigência contratual, de modo que eventual substituição da empresa prestadora dos serviços não comprometa a validade dos certificados emitidos, a ininterrupção das atividades institucionais ou a segurança dos atos praticados.

Além disso, a Administração deverá manter o controle sobre as informações necessárias à gestão da solução, assegurando que eventual migração para outro





fornecedor possa ocorrer de forma planejada, com preservação da integridade das informações, da estabilidade e regularidade dos serviços e da compatibilidade com os sistemas institucionais.

2.6 Direitos de Propriedade Intelectual e Autorais

Considerando que o objeto da presente contratação consiste na prestação de serviços de validação e emissão de certificados digitais, não envolvendo o desenvolvimento de software, criação de obras intelectuais, produção de código-fonte ou elaboração de produtos sujeitos à proteção por direitos autorais ou propriedade intelectual em favor do Tribunal, não se identificam, em regra, requisitos específicos relacionados à cessão de direitos de propriedade intelectual.

Entretanto, a futura contratação deverá assegurar ao Tribunal o pleno direito de utilização de todos os produtos, documentos, relatórios e demais artefatos eventualmente produzidos no âmbito da execução contratual, exclusivamente para fins institucionais, observadas as condições estabelecidas no Termo de Referência e na legislação aplicável.

2.7 Não Participação de Pessoas Físicas Consoante Instrução Normativa

Seges/Me n. 116/2021:

Esta contratação não é destinada à participação de pessoas físicas, devido aos seguintes motivos:

1. **Necessidade de Estrutura Empresarial e Credenciamento Regulatório:** O objeto compreende um escopo complexo e contínuo de validação documental, emissão criptográfica e custódia de identidades eletrônicas (e-CPFs) sob as regras estritas da ICP-Brasil. A execução eficiente da solução exige credenciamento formal perante o ITI como Autoridade Certificadora, Autoridade de Registro ou entidade tecnicamente habilitada, além de estrutura corporativa capaz de assegurar prepostos habilitados, plataformas em nuvem, logística de mídias, suporte técnico e continuidade operacional.
2. **Garantia de Ininterrupção e Nível de Serviço (SLA):** A sustentação dos mecanismos de assinatura digital e acesso aos sistemas essenciais do PJMT requer garantias de suporte ininterrupto, manutenção de postos de atendimento físicos em Cuiabá/MT e Várzea Grande/MT, e cumprimento de rigorosos prazos de





atendimento (SLA) que dependem do *know-how* e da solidez operacional exclusivos de pessoas jurídicas.

3. **Impacto Econômico e Encargos Previdenciários:** A admissão de propostas de pessoas físicas exigiria o acréscimo do encargo patronal de 20%(vinte por cento) de contribuição à Seguridade Social sobre o valor dos serviços para fins de julgamento. Diante da magnitude, volumetria e complexidade do objeto, tal estrutura de custos tornaria a contratação economicamente desvantajosa e ineficiente para a Administração Pública.
4. **Origem dos Recursos Financeiros:** O recurso financeiro para esta contratação não é advindo da União, portanto, não é obrigatória a participação de pessoas físicas, conforme art. 3º do Capítulo I das Disposições Preliminares da Instrução Normativa SEGES/ME nº 116/2021:

Art. 3º Os órgãos e entidades da Administração Pública estadual, distrital ou municipal, direta ou indireta, quando executarem recursos da União decorrentes de transferências voluntárias, deverão observar as regras desta Instrução Normativa.

Portanto, resta demonstrado no planejamento desta contratação que a mitigação de riscos operacionais e o alcance dos resultados pretendidos dependem estritamente da participação de pessoas jurídicas.

3. ESTRATÉGIA PARA A CONTRATAÇÃO

3.1 Natureza do Objeto

O objeto da presente contratação consiste na prestação de serviços comuns de Tecnologia da Informação e Comunicação (TIC), compreendendo a validação e emissão de certificados digitais Cert-JUS A3 para pessoa física, nas modalidades em nuvem e em mídia criptográfica (token USB), bem como a prestação de serviços correlatos necessários ao gerenciamento do ciclo de vida dos certificados.





Trata-se de serviço de natureza continuada, cuja interrupção poderá comprometer a continuidade das atividades jurisdicionais e administrativas do Tribunal de Justiça do Estado de Mato Grosso, especialmente aquelas que dependem de autenticação, assinatura eletrônica e acesso seguro aos sistemas institucionais.

Os serviços possuem padrões de desempenho e qualidade objetivamente definidos pelo mercado, pelas normas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), da cadeia Cert-JUS e pelas especificações estabelecidas neste Estudo Técnico Preliminar e no futuro Termo de Referência, caracterizando-se como serviços comuns, nos termos da Lei nº 14.133/2021.

A execução ocorrerá sob demanda, conforme as necessidades da Administração, sem dedicação exclusiva de mão de obra, sendo remunerados apenas os serviços efetivamente solicitados e executados.

3.2 Parcelamento e Adjudicação do Objeto

Nos termos do art. 40, inciso V, alínea "b", da Lei nº 14.133/2021, foi avaliada a possibilidade de parcelamento da solução, concluindo-se que não é técnica nem economicamente vantajosa a sua divisão, razão pela qual a contratação será realizada por lote único, com adjudicação a um único fornecedor.

A solução é composta pelos seguintes itens:

Item	Descrição
1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses para pessoa física, sem fornecimento de mídia criptográfica.
2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses para pessoa física, com fornecimento de mídia criptográfica (token USB).
3	Serviço de Visita Técnica para Emissão de Certificados Digitais

Embora representem itens distintos para fins de especificação, estimativa de consumo e faturamento, os três itens compõem uma única solução de certificação digital, destinada ao atendimento das necessidades do Poder Judiciário do Estado de Mato Grosso.

A solução foi concebida em modelo híbrido, contemplando certificados digitais Cert-JUS A3 em nuvem e certificados digitais Cert-JUS A3 com mídia criptográfica (token USB), permitindo a utilização da modalidade mais adequada conforme o perfil do





usuário, os requisitos técnicos dos sistemas utilizados e as necessidades operacionais da Administração. As visitas técnicas constituem atividade acessória e complementar à solução, sendo realizadas exclusivamente quando houver necessidade de atendimento presencial para validação de identidade, emissão, ativação, renovação, revogação, substituição ou suporte aos certificados digitais.

Os três itens apresentam elevado grau de integração funcional e operacional, uma vez que compartilham o mesmo fluxo de execução, iniciado com a autorização da emissão pela Administração, seguido da validação da identidade do usuário, emissão do certificado digital, disponibilização da credencial, ativação, suporte técnico e eventual renovação, revogação ou substituição. A distinção entre os dois primeiros itens reside apenas na forma de disponibilização do certificado — em nuvem ou em mídia criptográfica — permanecendo comuns todos os demais procedimentos necessários à prestação do serviço.

O parcelamento da contratação poderia resultar na execução desses serviços por fornecedores distintos, ocasionando dificuldades na coordenação das atividades, aumento dos custos administrativos de gestão e fiscalização, sobreposição ou indefinição de responsabilidades, além de riscos à continuidade da prestação do serviço, especialmente nas situações que demandem atuação integrada entre emissão, suporte técnico e atendimento presencial.

Além disso, a contratação de fornecedores distintos dificultaria o gerenciamento do ciclo de vida dos certificados digitais, exigindo diferentes canais de atendimento, processos distintos para emissão, renovação, revogação, suporte técnico e controle das solicitações, comprometendo a padronização dos procedimentos, a rastreabilidade das atividades e a eficiência operacional da Administração.

Sob o aspecto mercadológico, verifica-se que o mercado de certificação digital é composto por empresas aptas a fornecer, de forma integrada, as diferentes modalidades de certificados digitais Cert-JUS, com e sem mídia criptográfica, bem como os serviços de validação, emissão e atendimento presencial necessários à sua execução. Inclusive, em pesquisa de soluções similares, constatou-se que diversos órgãos da Administração Pública, especialmente do Poder Judiciário, estruturaram suas contratações contemplando, em um único lote, os serviços de emissão e validação de certificados digitais, fornecimento de dispositivos criptográficos e serviços de atendimento presencial,





evidenciando que essa forma de contratação é compatível com as práticas adotadas pelo mercado e não implica restrição à competitividade.

Dessa forma, conclui-se que a adjudicação por lote único representa a alternativa mais vantajosa para a Administração, por assegurar a integração da solução, a centralização da responsabilidade pela execução contratual, maior eficiência na gestão e fiscalização do contrato, padronização dos procedimentos operacionais, simplificação do atendimento aos usuários, redução dos riscos de descontinuidade dos serviços e maior efetividade na execução do objeto, em observância aos princípios da eficiência, da economicidade, do planejamento, da competitividade e da obtenção da proposta mais vantajosa, previstos na Lei nº 14.133/2021.

3.3 Modalidade e Tipo de Licitação

A contratação pretendida refere-se ao Registro de Preços para futura e eventual contratação de empresa especializada na prestação de serviços de validação e emissão de certificados digitais e-CPF (Cadeia Cert-JUS A3) para pessoa física, nas modalidades em nuvem e com fornecimento de mídia criptográfica, contemplando, ainda, visitas técnicas sob demanda. Os serviços são amplamente disponibilizados por empresas especializadas no mercado de Tecnologia da Informação e Comunicação (TIC). Dessa forma, o objeto enquadra-se como bens e serviços comuns de TIC e, portanto, licitação via Pregão, em sua forma eletrônica, com finalidade de aquisição, pelo menor preço global, previamente ao menor preço individual de cada item do lote, e modo de disputa aberto e fechado.

3.4 Classificação e Indicação Orçamentária

Unidade Orçamentária: 03.601 Funajuris.

Unidade Gestora – UG: 0001 e 0002.

Fonte: 1.760.0000/2.760.0000

Natureza: 3.3.90.40

Ação (P/A/OE): 2009- Manutenção de ações de informática.

Programa: 036 – Apoio Administrativo.

A contratação será para 1ª e 2ª instância.





3.5 Das implicações da forma de pagamento

Tabela 11 – Formas de pagamento

Item	Descrição	Forma de Pagamento
1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses para pessoa física, sem fornecimento de mídia criptográfica.	Mensal, por aferição (sob demanda): Pagamento realizado com base no quantitativo de certificados efetivamente validados, emitidos e homologados pela Fiscalização no mês de referência, mediante a conferência dos relatórios extraídos do sistema da contratada e confrontados com os vouchers/autorizações emitidos pelo PJMT. O valor estará sujeito a readequações financeiras decorrentes da aplicação do Instrumento de Medição de Resultado (IMR).
2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses para pessoa física, com fornecimento de mídia criptográfica (token USB).	Mensal, por aferição (sob demanda): Pagamento realizado por solução integrada entregue (serviço de emissão + hardware do token), considerando apenas as unidades efetivamente emitidas e recebidas pelos usuários no mês anterior. A liberação do pagamento fica condicionada à entrega dos dispositivos em perfeita conformidade técnica, sem custos logísticos adicionais e com a devida ativação assistida, sujeitando-se às glosas do IMR em caso de atrasos na entrega ou falhas no hardware.
3	Serviço de Visita Técnica para Emissão de Certificados Digitais.	Por evento realizado (sob demanda): Pagamento efetuado mensalmente com base no número de visitas técnicas efetivamente executadas e concluídas nas comarcas/unidades demandadas. Cada visita deverá estar respaldada por Ordem de Serviço prévia da Fiscalização e acompanhada do respectivo Termo de Encerramento/Relatório de Atendimento assinado pelo responsável local, atestando a resolução do chamado.

3.6 Vigência dos bens e/ou serviços

Esclarece-se que a vigência da Ata de Registro de Preços observará o prazo previsto no art. 84 da Lei nº 14.133/2021, enquanto os contratos dela decorrentes poderão ter vigência própria, conforme a natureza continuada dos serviços e as disposições do art. 107 da mesma Lei, observadas as condições estabelecidas no Termo de Referência.





A vigência do contrato será de 24 (vinte e quatro) meses, podendo ser prorrogado nos termos do Artigo 107 da referida Lei 14.133/2021.

A data de início do contrato ocorrerá quando da assinatura de ambas as partes, a qual será objeto de Certidão aposta pela Coordenadoria Administrativa – Departamento Administrativo nos autos.

A escolha do prazo de vigência baseia-se:

- A definição desse prazo considera a validade prevista para os certificados digitais a serem contratados, correspondente a 24 (vinte e quatro) meses, permitindo que a execução contratual acompanhe integralmente o ciclo de vida dos certificados digitais emitidos, sem necessidade de renovações intermediárias durante o período contratado.
- A vigência contratual também se mostra adequada para permitir a adoção gradual do certificado digital em nuvem no âmbito da CONTRATANTE, considerando que a solução representa evolução em relação ao modelo tradicional baseado em mídia física, token USB. Essa transição poderá ocorrer de forma progressiva, conforme a aceitação dos usuários, os resultados dos testes de compatibilidade, a maturidade operacional da solução, a adaptação dos fluxos internos e a necessidade de ininterrupção dos serviços judiciais e administrativos.
- Durante esse período, a CONTRATANTE poderá avaliar a experiência de uso do certificado em nuvem, sua compatibilidade com os sistemas institucionais, a efetividade da autenticação forte, a redução da dependência de mídias físicas, os ganhos operacionais e eventuais ajustes necessários para ampliação da adoção da solução, sem prejuízo do suporte ininterrupto e do fornecimento de certificados físicos quando necessários.
- O prazo dilatado permitirá obtenção de ganho de escala, reduzindo o grau de incerteza da contratação e consequentemente melhores preços para a Administração;
- Seguindo esta lógica, a jurisprudência do Tribunal de Contas da União sustenta a possibilidade da fixação do prazo de vigência estendido com a finalidade de obter preços e condições mais vantajosos para a Administração, (Acórdão 3.320/2013-Segunda Câmara):





“O prazo de vigência de contratos de serviços contínuos deve ser estabelecido considerando-se as circunstâncias de forma objetiva, fazendo-se registrar no processo próprio o modo como interferem na decisão e quais suas consequências. Tal registro é especialmente importante quando se fizer necessário prazo inicial superior aos doze meses entendidos como regra pelo TCU. Há necessidade de se demonstrar o benefício decorrente do prazo estabelecido (Acórdão 3320/2013-Segunda Câmara).” Um prazo contratual exíguo implicaria na constante dedicação de recursos humanos especificamente para processos de Planejamento da Contratação, considerando que os trabalhos de renovação/prorrogação são deflagrados com pelo menos 180 dias de antecedência (em atendimento à recomendação do Tribunal de Contas da União esposada no Acórdão nº 728/2008 – 1ª Câmara);”

3.7 Equipe de Apoio à Contratação

Área Demandante

Identificação da Área Demandante: Departamento de Suporte e Informação

- **Responsável pela Área Demandante:** Marcos Pinto Gomes Júnior
- **Matrícula:** 5851
- **E-mail:** marcos.gomes@tjmt.jus.br

Integrante Demandante

- **Nome:** Marcos Pinto Gomes Júnior
- **Matrícula:** 5851
- **E-mail:** marcos.gomes@tjmt.jus.br

Integrante Demandante Substituto

- **Nome:** Ângela Maria Franchini





- **Matrícula:** 7949
- **E-mail:** angela.franchini@tjmt.jus.br

Integrante Técnico

- **Nome:** Jefferson de Mattos Domingos
- **Matrícula:** 6117
- **E-mail:** jefferson.domingos@tjmt.jus.br

Integrante Técnico Substituto

- **Nome:** Thiago Apolonio De Assunção Silva
- **Matrícula:** 45838
- **E-mail:** thiago.silva@tjmt.jus.br

Integrante Administrativo

- **Nome:** Moacyr José Couto Daima Filho
- **Matrícula:** 37465
- **E-mail:** moacyr.filho@tjmt.jus.br

Integrante Administrativo Substituto

- **Nome:** Fábio Carlos Arruda da Silva
- **Matrícula:** 38556
- **E-mail:** fabio.arruda@tjmt.jus.br

Autoridade Máxima de TIC

- **Nome:** Marcia Regina de Carvalho Buhr
- **Matrícula:** 55940
- **E-mail:** marcia.buhr@tjmt.jus.br

4. ANÁLISE DE RISCOS

Em atenção ao artigo 18, inciso X, da Lei Federal nº 14.133/2021, que destaca a importância da gestão de riscos para o sucesso da licitação e execução contratual, bem como ao artigo 10 da Resolução CNJ nº 468/2022, que prevê ações de gerenciamento de riscos e a elaboração do mapa de gerenciamento, e que este deve ser juntado ao processo de contratação após a elaboração dos Estudos Técnicos Preliminares.





É importante mencionar que, conforme disposto no artigo 22 da Lei Federal nº 14.133/2021, o edital poderá contemplar matriz de alocação de riscos entre o contratante e o contratado, hipótese em que o cálculo do valor estimado da contratação poderá considerar taxa de risco compatível com o objeto da licitação e com os riscos atribuídos ao contratado, de acordo com metodologia predefinida pelo ente federativo.

De acordo com o art. 22, § 3º da Lei Federal nº 14.133/2021, para contratações de grande vulto, é obrigatório que o edital inclua o Mapa de Gerenciamento de Riscos, que aloca os riscos entre o contratante e o contratado. Para contratações de menor vulto, a exigência desse artefato fica a critério do órgão, que deve definir o valor estimado para a não exigência do mesmo.

Dessa forma, é ressaltada a importância da elaboração do mapa de gerenciamento de risco, sua criação dependerá de critérios e valores mínimo definidos por normativo específico de cada órgão.

Neste tópico, são assinalados os principais riscos detectados envolvidos no planejamento da contratação e na gestão do contrato.

4.1 Riscos Mapeados

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste Estudo Técnico Preliminar:

PCTIC – Planejamento da Contratação;

SFTIC – Seleção de Fornecedores;

GCTIC – Gestão do Contrato.

Abaixo a classificação escalar da probabilidade e do impacto, conforme a tabela de referência a seguir:

Classificação	Valor
Baixo	5
Médio	10
Alto	15

Escala de Classificação de Probabilidade e Impacto

A tabela a seguir apresenta a Matriz de Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

	15	75	150	225
--	----	----	-----	-----





PROBABILIDADE (P)	10	50	100	150
	5	25	50	75
		5	10	15
	IMPACTO (I)			

Figura: Matriz de Probabilidade x Impacto

A probabilidade está associada às chances do evento acontecer e cause um impacto negativo.

O impacto está associado às consequências do evento ocorrido caso o risco se materialize.

1 - IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS					
A tabela a seguir apresenta uma síntese dos riscos identificados e classificados nesse documento.					
ID	RISCO	RELACIONADO AO (À):	P2	I3	NÍVEL DE RISCO (PxI)
1	Escolha inadequada da solução tecnológica	Planejamento da Contratação	5	15	75
2	Dimensionamento incorreto da demanda.	Planejamento da Contratação	5	15	75
3	Risco de contingenciamento de recursos orçamentários antes da contratação	Planejamento da Contratação	10	15	150
4	Ausência de recursos orçamentários ou financeiros	Planejamento da Contratação	10	15	150
5	Não aprovação dos artefatos do Planejamento da Contratação	Planejamento da Contratação	5	10	50
6	Deficiência na pesquisa de preços	Planejamento da Contratação	5	15	75
7	Atraso na conclusão do planejamento da contratação	Planejamento da Contratação	15	15	225
8	Atraso na análise jurídica	Planejamento da Contratação	10	15	150
9	Incompatibilidade técnica da solução com sistemas judiciais/administrativos (PJe, PJeOffice, etc.)	Planejamento da Contratação	5	15	75
10	Não cumprimento dos requisitos normativos (ICP-Brasil, Cert-JUS, LGPD, CNJ)	Planejamento da Contratação	5	15	75
11	Contratada se recusar a assinar o contrato	Gestão Contratual	5	10	50
12	Incapacidade da empresa contratada de execução do contrato	Gestão Contratual	5	15	75





13	Atraso no pagamento de serviços prestados	Gestão Contratual	5	15	75
14	Suspensão pela má prestação dos serviços	Gestão Contratual	5	15	75
15	Vazamento de dados e informações pela contratada	Gestão Contratual	5	15	75
16	Qualificação técnica e operacional insuficientes dos fiscais técnicos do contrato	Gestão Contratual	5	15	75
17	Falhas na emissão, ativação, leitura ou utilização dos certificados e tokens	Gestão Contratual	10	15	150
18	Comprometimento da segurança da informação e das chaves criptográficas	Gestão Contratual	5	15	75
19	Risco logístico no envio, atraso ou extravio dos tokens físicos	Gestão Contratual	10	10	100
20	Atraso no atendimento, suporte técnico ou realização de visita técnica presencial	Gestão Contratual	10	15	150
21	Baixa adesão ou dificuldade de adaptação dos usuários ao certificado em nuvem	Gestão Contratual	10	10	100

Legenda: P – Probabilidade; I – Impacto.

2 - AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS		
RISCO 01	Escolha inadequada da solução tecnológica	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Termo de Referência deficiente	
DANO 2:	Baixa qualidade do serviço contratado	
DANO 3:	Utilização de solução antieconômica	
Tratamento:	Prevenir	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Capacitar a equipe que elabora a especificação	CTI
02	Realização de estudos comparativos entre soluções	Equipe técnica do Planejamento da Contratação (EPC)
03	Elaboração de ETP aprofundado sobre a temática	Equipe técnica do Planejamento da Contratação (EPC)
04	Fazer pesquisas no mercado	Equipe técnica do Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





05	Revisão dos artefatos de planejamento	Equipe de Planejamento da Contratação (EPC)
06	Reiniciar a contratação	Núcleo de Aquisições-CTI

RISCO 02	Dimensionamento incorreto da demanda	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Atraso na conclusão do processo de contratação	
DANO 2:	Recursos públicos utilizados com baixa eficiência	
DANO 3:	Contrato insuficiente para atender às necessidades do órgão	
Tratamento:	Prevenir	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Efetuar estudo detalhado de estimativa atual e futura	Equipe técnica do Planejamento da Contratação (EPC)
02	Pesquisar contratações similares, mapear cenários compatíveis e verificar junto aos contratantes as principais dificuldades	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Propor aditivo ou supressão contratual para ajustar à necessidade real	Equipe de Planejamento da Contratação (EPC)
04	Readequar especificações de acordo com critérios ou modelos mais conservadores	Equipe de Planejamento da Contratação (EPC)

RISCO 03	Risco de contingenciamento de recursos orçamentários antes da contratação	
PROBABILIDADE:	Média	
IMPACTO:	Alto	
DANO 1:	Atraso no processo	
DANO 2:	Suspensão na prestação do serviço	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Certificar-se da existência de recursos financeiros compatíveis com a solução pretendida	Núcleo de Aquisições-CTI
02	Realizar reunião com as áreas afins para garantir a priorização de recursos	Núcleo de Aquisições-CTI
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





03	Revisar a capacidade planejada para cada contrato e refazer o planejamento de acordo com o orçamento disponível	Equipe de Planejamento da Contratação (EPC)
----	---	---

RISCO 04	Ausência de recursos orçamentários ou financeiros	
PROBABILIDADE:	Média	
IMPACTO:	Alto	
DANO 1:	Suspensão da prestação do serviço	
DANO 2:	Adiamento da contratação do serviço	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Diálogo prévio e gestão junto às áreas responsáveis com vistas ao provimento dos recursos necessários à contratação	Núcleo de Aquisições-CTI
02	Reserva de recursos financeiros	Núcleo de Aquisições-CTI
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Prover meios para viabilização da contratação, promovendo ações junto à alta administração visando a obtenção de recursos para a contratação pretendida	Núcleo de Aquisições-CTI

RISCO 05	Não aprovação dos artefatos do planejamento da contratação	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Atraso no processo de contratação	
DANO 2:	Suspensão da prestação do serviço	
Tratamento:	Prevenir	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Reuniões com autoridades superiores para alinhamento e aprovação dos artefatos	Equipe de Planejamento da Contratação (EPC);
02	Revisão minuciosa dos artefatos pela equipe de planejamento da contratação	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Convocação de reuniões da equipe de planejamento para realização dos ajustes necessários para encaminhamento do processo	Equipe de Planejamento da Contratação (EPC)

RISCO 06	Deficiência na pesquisa de preços	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	





DANO 1:	Obtenção de preços excessivamente elevados	
DANO 2:	Obtenção de preços inexequíveis	
DANO 3:	Prejuízo ao erário	
Tratamento:	Prevenir	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Realizar procedimento de estimativa de preços durante a elaboração do Estudo Técnico Preliminar	Equipe de Planejamento da Contratação (EPC)
02	Utilização de diversas ferramentas para obtenção de preços públicos, como por exemplo, Planilhas de bens e serviços de TIC; Pannel de preços; Portal de Compras Governamentais (Comprasnet); Contratos similares	Equipe de Planejamento da Contratação (EPC)
03	Exclusão dos preços inexequíveis ou excessivamente elevados utilizando os critérios fixados pela Portaria nº 804 - MJ, de 13 de novembro de 2018	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
04	Justificativas obrigatórias para quando não houver a possibilidade de obtenção de pelo menos três preços exequíveis ou fornecedores, conforme § 6º do art. 2º da IN 03/2017	Equipe de Planejamento da Contratação (EPC) e aprovação pela autoridade competente (CTI)
05	Revogar o processo de aquisição e realização de novo processo licitatório	Equipe de Planejamento da Contratação (EPC)

RISCO 07	Atraso na conclusão do planejamento da contratação	
PROBABILIDADE:	Alta	
IMPACTO:	Alto	
DANO 1:	Atraso na conclusão do processo	
DANO 2:	Suspensão da prestação do serviço	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Alocação tempestiva da equipe de planejamento da contratação	Autoridades competentes das áreas técnica, administrativa e requisitante.
02	Definição e cumprimento de cronograma de atividades pelos integrantes e alocação em tempo integral dos atores para conclusão da etapa de planejamento	Equipe de Planejamento da Contratação (EPC); autoridades competentes das áreas técnica, administrativa e requisitante.
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





03	Retirar a prioridade de outras ações para liberação dos integrantes da EPC para a atividade de planejamento da contratação.	Autoridades competentes das áreas técnica, administrativa e requisitante;
----	---	---

RISCO 08	Atraso na análise jurídica	
PROBABILIDADE:	Média	
IMPACTO:	Alto	
DANO 1:	Atraso na contratação	
DANO 2:	Suspensão da prestação do serviço	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Verificar junto à Assessoria Jurídica a possibilidade de agilização da análise para este projeto	Núcleo de Aquisições-CTI
02	Revisar os documentos de acordo com as recomendações recentes da área jurídica, de modo a facilitar análise e minimizar necessidade de alterações posteriores	Equipe de Planejamento da Contratação (EPC); Setor de licitações e contratos
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Retirar a prioridade de outras ações para liberação dos integrantes da EPC para a atividade de planejamento da contratação	Autoridades competentes das áreas técnica, administrativa e requisitante;

RISCO 09	Incompatibilidade técnica da solução com os sistemas judiciais e administrativos utilizados pela CONTRATANTE (incluindo PJe, PJeOffice, assinadores digitais, navegadores, sistemas operacionais, aplicações corporativas e plataformas do PJMT/CNJ).	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Paralisação na assinatura de peças jurídicas e despachos processuais.	
DANO 2:	Inutilização prática dos certificados adquiridos.	
DANO 3:	Atrasos na prestação jurisdicional.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Definir rigorosamente no ETP e TR os critérios e requisitos de compatibilidade técnica exigidos.	Equipe de Planejamento da Contratação (EPC);
02	Prever em edital a obrigatoriedade de uma fase de Prova de Conceito (PoC) e testes de compatibilidade antes da homologação.	Equipe de Planejamento da Contratação (EPC);
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





01	Realizar testes imediatos com a emissão de certificados de teste (físicos e em nuvem) fornecidos pela licitante.	Equipe Técnica / CTI
02	Reprovar a solução da empresa caso seja constatada a incompatibilidade intransponível nos testes.	Equipe Técnica / CTI

RISCO 10	Não cumprimento dos requisitos normativos (ICP-Brasil, Cert-JUS, LGPD, CNJ)	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Invalidade jurídica de assinaturas digitais efetuadas sob a vigência do contrato.	
DANO 2:	Aplicação de sanções administrativas ou processos judiciais contra o órgão.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Exigir no Termo de Referência a comprovação de conformidade normativa e o credenciamento como Prestador de Serviço de Confiança (PSC), quando aplicável.	Equipe de Planejamento da Contratação (EPC)
02	Exigir a apresentação de documentação técnica oficial, relatórios de auditoria e mecanismos de rastreabilidade.	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
02	Reprovar ou rescindir a contratação da solução em caso de não conformidade identificada na fase de homologação ou na execução do contrato.	Equipe de gestão e fiscalização contratual

RISCO 11	Contratada se recusar a assinar o contrato	
PROBABILIDADE:	Baixa	
IMPACTO:	Médio	
DANO 1:	Indisponibilidade dos serviços contratados	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Definir punição no Termo de Referência para o descumprimento de cláusula que prevê a assinatura do contrato em determinado prazo	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
02	Aplicar as punições previstas no Termo de Referência e Contrato	Equipe de gestão e fiscalização contratual

RISCO 12	Incapacidade da empresa contratada de execução do contrato	
PROBABILIDADE:	Baixa	





IMPACTO:	Alto	
DANO 1:	Indisponibilidade dos serviços contratados	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Incluir no Termo de Referência níveis mínimos de serviços, sanções e os requisitos de qualidade que sejam condizentes com a importância dos serviços a serem prestados	Equipe de Planejamento da Contratação (EPC)
02	Exigir da Contratada a prestação de garantia contratual, permitida em lei, com vistas a assegurar o compromisso da empresa na prestação adequada dos serviços	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Fiscalização do contrato com aplicação de sanções previstas quando ocorrer alguma falha contratual e, em último caso, cancelar contrato	Equipe de gestão e fiscalização contratual;

RISCO 13	Atraso no pagamento de serviços prestados	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Suspensão da prestação do serviço	
DANO 2:	Rescisão contratual por falta de pagamento	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Estabelecer, de forma bastante clara no Termo de Referência, as medidas compensatórias a que a empresa faz jus em caso de atrasos no pagamento de serviços prestados e atestados	Equipe de Planejamento da Contratação (EPC)
02	Atuar, junto a alta administração, para que não falte recurso para o pagamento dos serviços prestados	Gestor do Contrato;
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Ao menor sinal de contingenciamento de recursos, notificar a contratada sobre o ocorrido e contingenciar ordens de serviço, quando necessário, para que o fornecedor possa ajustar sua operação e garantir o nível mínimo de serviço eventualmente estabelecido.	Equipe de gestão e fiscalização do contrato;
04	Estabelecer contato regular com os gestores da contratada para, caso seja necessário, entrar em nível mínimo de serviço e evitar o colapso financeiro da contratada	Equipe de gestão e fiscalização do contrato;

RISCO 14	Suspensão pela má prestação dos serviços
PROBABILIDADE:	Baixa





IMPACTO:	Alto	
DANO 1:	Indisponibilidade dos serviços contratados	
DANO 2:	Se não sanadas as falhas, pode ensejar uma rescisão contratual	
Tratamento:	Prevenir	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Estabelecer no Termo de Referência, os níveis de serviços a serem cumpridos e as sanções aplicáveis em caso de má prestação dos serviços	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
02	Fiscalização do contrato com aplicação de sanções previstas em lei e no Termo de Referência	Equipe de gestão e fiscalização contratual

RISCO 15	Vazamento de dados e informações pela contratada	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Reputação, imagem e credibilidade afetadas negativamente	
DANO 2:	Interrupção do negócio	
DANO 3:	Demandas judiciais por eventuais prejuízos	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Incluir no Termo de Referência a obrigação da empresa em assinar os termos de compromisso de manutenção de sigilo e de ciência	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
02	Fiscalização do contrato com aplicação de sanções previstas em lei e no Termo de Referência	Equipe de gestão e fiscalização contratual

RISCO 16	Qualificação técnica e operacional insuficientes dos fiscais técnicos do contrato	
PROBABILIDADE:	Baixa	
IMPACTO:	Médio	
DANO 1:	Fragilidades no planejamento, gestão e fiscalização contratual, que poderão gerar resultados equivocados e risco de pagamentos indevidos à empresa.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Caso seja necessário, providenciar a capacitação dos servidores que irão desempenhar o papel de fiscal técnico	Equipe de gestão e fiscalização contratual
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





02	Retirar a prioridade de outras ações para liberação de recursos humanos capacitados para a realização da fiscalização contratual	Autoridades responsáveis pelas áreas de fiscalização técnica
----	--	--

RISCO 17	Falhas na emissão, ativação, leitura ou utilização dos certificados e tokens	
PROBABILIDADE:	Média	
IMPACTO:	Alto	
DANO 1:	Indisponibilidade de uso do certificado pelo usuário final.	
DANO 2:	Acumulação de chamados técnicos na equipe de suporte interno do órgão.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Estabelecer cláusulas contratuais rígidas com prazos de SLA/IMR específicos para suporte e correção de falhas.	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
02	Acionar o suporte técnico da CONTRATADA para a realização de correções, reemissões, substituições ou regularizações necessárias.	Equipe de gestão e fiscalização contratual
03	Manter registro detalhado de todos os atendimentos e falhas para aplicação de sanções em caso de descumprimento de prazos.	Fiscal do Contrato

RISCO 18	Comprometimento da segurança da informação e das chaves criptográficas (tentativa de acesso indevido, uso não autorizado, comprometimento de senha/PIN, dispositivo ou credenciais).	
PROBABILIDADE:	Baixa	
IMPACTO:	Alto	
DANO 1:	Assinatura de documentos por terceiros de forma fraudulenta.	
DANO 2:	Quebra de sigilo e integridade das informações institucionais.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Exigir que a solução assegure a proteção das chaves privadas, vedação à exportação/cópia e criptografia em trânsito.	Equipe de Planejamento da Contratação (EPC)
02	Implementar mecanismos de autenticação forte, controle de acessos e trilhas de auditoria.	CTI / Área de Segurança da Informação
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





03	Solicitar a revogação imediata do certificado digital afetado junto à Autoridade Certificadora.	Titular do Certificado / Fiscal do Contrato
04	Auditar as trilhas de registro de acessos para identificar a origem do comprometimento.	CTI / Segurança da Informação

RISCO 19	Risco logístico no envio dos tokens físicos (atraso, extravio, entrega em endereço incorreto, dano no transporte ou falha na rastreabilidade).	
PROBABILIDADE:	Média	
IMPACTO:	Médio	
DANO 1:	Atraso no início das atividades operacionais dos novos servidores.	
DANO 2:	Extravio de patrimônio público (tokens adquiridos).	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Atribuir contratualmente à CONTRATADA a total responsabilidade pela logística de envio, embalagem, postagem e rastreamento.	Equipe de Planejamento da Contratação (EPC)
02	Inserir no Termo de Referência o Anexo específico com as regras de logística e os endereços formais da CONTRATANTE.	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
03	Exigir a regularização de eventuais falhas de entrega com base nas informações atualizadas do ticket/voucher.	Equipe de gestão e fiscalização contratual
04	Cobrar a reposição imediata de mídias danificadas ou extraviadas sem custos adicionais para o órgão.	Equipe de gestão e fiscalização contratual

RISCO 20	Atraso no atendimento, suporte técnico ou realização de visita técnica presencial	
PROBABILIDADE:	Média	
IMPACTO:	Alto	
DANO 1:	Prolongamento do tempo de indisponibilidade do usuário.	
DANO 2:	Desgaste operacional nas secretarias e comarcas dependentes do certificado.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Definir contratualmente prazos objetivos, indicadores de medição de resultados, severidades e SLA/IMR.	Equipe de Planejamento da Contratação (EPC)
02	Impor a obrigação de atualização de todos os registros e chamados na ferramenta oficial da CONTRATANTE.	Equipe de Planejamento da Contratação (EPC)
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL





03	Aplicar penalidades e glosas contratuais proporcionais ao atraso verificado no atendimento.	Equipe de gestão e fiscalização contratual
04	Exigir a execução imediata de um plano de ação corretivo por parte da CONTRATADA.	Equipe de gestão e fiscalização contratual

RISCO 21	Baixa adesão ou dificuldade de adaptação dos usuários ao certificado em nuvem por representar uma mudança gradual em relação ao modelo tradicional baseado em token físico.	
PROBABILIDADE:	Média	
IMPACTO:	Médio	
DANO 1:	Resistência cultural dos usuários e subutilização da tecnologia adquirida.	
DANO 2:	Erros operacionais frequentes na ativação e autorização de dispositivos.	
Tratamento:	Mitigar	
ID:	AÇÃO PREVENTIVA	RESPONSÁVEL
01	Planejar a implantação do certificado em nuvem de forma progressiva e faseada no órgão.	Equipe de gestão e fiscalização contratual
02	Prever ações de orientação, manuais práticos e acompanhamento próximo da experiência de uso dos usuários.	Equipe de gestão e fiscalização contratual
03	Manter a opção de fornecimento de certificado físico (token) para casos de necessidade comprovada.	Equipe de gestão e fiscalização contratual
ID:	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
04	Disponibilizar plantões de suporte dedicados para mitigar dúvidas recorrentes no período de transição.	Equipe de gestão e fiscalização contratual

5. APROVAÇÃO E ASSINATURA

Equipe de Planejamento da Contratação, instituída pelo DOD-12/2026-NC, bem como pela autoridade competente da área de TIC, aprovam o presente Estudo Técnico Preliminar e atestam sua conformidade às disposições da Resolução CNJ nº 468/2022.

ÁREA DEMANDANTE – DEPARTAMENTO DE SUPORTE E INFORMAÇÃO	
INTEGRANTE/FISCAL DEMANDANTE	INTEGRANTE/FISCAL DEMANDANTE SUBSTITUTO





<u>Marcos Pinto Gomes Junior</u> marcos.gomes@tjmt.jus.br Matrícula: 5851	<u>Ângela Maria Franchini</u> angela.franchini@tjmt.jus.br Matrícula: 7949
ÁREA TÉCNICA	
INTEGRANTE/FISCAL TÉCNICO	INTEGRANTE/FISCAL TÉCNICO SUBSTITUTO
<u>Jefferson de Mattos Domingos</u> jefferson.domingos@tjmt.jus.br Matrícula: 6117	<u>Thiago Apolonio De Assunção Silva</u> thiago.silva@tjmt.jus.br Matrícula: 45838
INTEGRANTES ADMINISTRATIVOS	
FISCAL ADMINISTRATIVO	FISCAL ADMINISTRATIVO SUBSTITUTO
<u>Moacyr José Couto Daima Filho</u> Moacyr.filho@tjmt.jus.br Matrícula: 37465	<u>Fabio Carlos Arruda da Silva</u> Fabio.arruda@tjmt.jus.br Matrícula: 38556
AUTORIDADE MÁXIMA DA ÁREA DE TIC	
<u>Marcia Regina de Carvalho Buhr</u> Matrícula: 55940 Coordenadora de Tecnologia da Informação Cuiabá, 25 de agosto de 2026.	

6. CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

Confirmo o recebimento do Estudo Técnico Preliminar, no qual tomo ciência de forma integral de seu conteúdo. A partir deste momento, darei prosseguimento às providências cabíveis visando garantir o encaminhamento do ETP para a instância competente do órgão.





ANEXO A - LISTA DE POTENCIAIS FORNECEDORES

Certificado Digital Pessoa Física

Ressalta-se que a listagem de fornecedores é meramente exemplificativa.

Item	Fornecedor
1	Nome: AR RP Certificação Digital Ltda. Sítio: https://arrp.acsoluti.com.br/ Telefone: (62) 3414-9600 E-mail: licitacoes@rpcd.com.br
2	Nome: Certdata Certificadora Digital Sítio: https://certdata.com.br/ Telefone: 0800 580 8090 contato@certdata.com.br
3	Nome: Certisign Certificadora Digital S.A. Sítio: https://certisign.com.br/ Telefone: (11) 3478-9444 E-mail: licit@certisign.com.br
4	Nome: Digisec Certificação Digital Ltda. Sítio: https://digisec.com.br/ Telefone: (62) 3414-7250 E-mail: licitacoes@digisec.com.br
5	Nome: Iridia Soluções Ltda. Sítio: https://iridia.com.br Telefone: (31) 3500-0000 E-mail: contato@iridia.com.br
6	Nome: Prisminas Certificação Digital Ltda. Sítio: https://prisminascertificados.com.br/ Telefone: (37) 3229-1313 E-mail: certificadodigital@prisminas.com.br
7	Nome: Saldaris Consultoria e Serviços Ltda. Sítio: https://saldarisconsultoria.com.br/ Telefone: (47) 98921 – 4675 / (47) 8921 - 4675 E-mail: servicos@saldarisconsultoria.com.br
8	Nome: Safeweb Segurança da Informação Ltda. Sítio: https://safeweb.com.br/ Telefone: (51) 4042-1313 comercial@safeweb.com.br
9	Nome: Soluti Sítio: https://www.soluti.com.br/ Telefone: (62) 3412-0220 E-mail: licitacoes@objectti.com.br
10	Nome: Soma Estratégia Ltda. Sítio: https://somaestrategia.com.br/ Telefone: (79) 2106-6100 E-mail: licitacao@somaestrategia.com.br
11	Nome: Tech Minas Digital Ltda. Sítio: https://artechminasdigital.gestao.plus/loja/ Telefone: (37) 99929-3255 E-mail: techminasdigital@gmail.com
12	Nome: Valid Certificadora Digital Ltda. Sítio: https://validcertificadora.com.br/





Item	Fornecedor
	Telefone: (11) 2575-6918 E-mail: janaina.mattos@valid.com admingov@valid.com
13	Nome: X.Digital Brasil Segurança da Informação Ltda. Sítio: https://xdigitalbrasil.com.br/ Telefone: (62) 3517-9739 E-mail: contato@xdigitalbrasil.com.br
14	Nome: Zeferino & Camelo Serviços Administrativos Ltda. davoslicita@gmail.com 88 9651-7898





ANEXO B - CONTRATAÇÕES SIMILARES

Pregão Eletrônico n. 07/2026 do Tribunal de Justiça do Estado do Rio Grande do Norte



EDITAL

PREGÃO ELETRÔNICO Nº	07/2026 (90007/2026)
PROCESSO Nº	04101.008486/2025-37
DATA DE ABERTURA	14/05/2026 ÀS 14 HORAS (art. 55, I, "a", Lei nº 14.133/2021)
LOCAL	www.gov.br UASG Nº 925869
OBJETO:	Aquisição de vouchers para certificados digitais, visando atender à demanda do Poder Judiciário do Estado do Rio Grande do Norte (PJRN) por serviços de certificação digital, essenciais à validade jurídica dos atos processuais praticados nos sistemas judiciais eletrônicos.
FUNDAMENTAÇÃO:	Pela Lei nº 14.133/2021 ; pela IN 73/2022; pela Lei Complementar nº 123/2006; pela Lei nº 12.846/2013 – Decreto 11.129/2022 e Lei n. 13.709/2018 e demais normas correlatas que tratem da matéria.
TIPO DE LICITAÇÃO/CRITÉRIO DE JULGAMENTO:	MENOR PREÇO POR GRUPO ÚNICO
VALOR GLOBAL MÁXIMO ESTIMADO DA LICITAÇÃO	R\$ 1.207.616,80
LICITAÇÃO COM PARTICIPAÇÃO EXCLUSIVA DE MICROEMPRESA E EMPRESA DE PEQUENO PORTE PARA OS ITENS CUJO VALOR SEJA ATÉ 80.000,00 – LEI COMPLEMENTAR Nº 123/2006 E DEMAIS ALTERAÇÕES	NÃO
COTA RESERVADA	NÃO
REGISTRO DE PREÇOS	NÃO
VISTORIA	NÃO
PEDIDOS DE ESCLARECIMENTOS/IMPUGNAÇÕES	11/05/2026 para o email pregao@tjrn.jus.br
PRAZO PARA ENVIO DE PROPOSTA/DOCUMENTOS SOLICITADOS	Até 2 horas após a convocação (art. 29, § 2º da IN 73/2022), admitida prorrogação.
MODO DE DISPUTA	ABERTO COM LANCE MÍNIMO DE R\$ 5,00 (art. 57 da Lei nº 14.133/2021)





Pregão Eletrônico n. 11/2026 do Ministério Público do Estado de Mato Grosso



MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

Procuradoria-Geral de Justiça
Departamento de Aquisições
Gerência de Licitações
Pregão Eletrônico n.º 90011/2026

EDITAL

Pregão Eletrônico n.º 90011/2026 UASG: 926625		Data de Abertura: 07/05/2026 às 09h30min No sítio www.gov.br/compras	
Objeto			
REGISTRO DE PREÇOS PARA FUTURA E EVENTUAL AQUISIÇÃO DE CERTIFICADOS DIGITAIS (E-CPF E E-CNPJ), NO PADRÃO ICP-BRASIL E DIÁRIAS DE VALIDAÇÃO PRESENCIAL, DE ACORDO COM AS CONDIÇÕES, ESPECIFICAÇÕES E QUANTIDADES DESCRITAS NO TERMO DE REFERÊNCIA – ANEXO I DO EDITAL.			
Registro de Preços?	Vistoria	Instrumento Contratual	Modo de Disputa
SIM	NÃO	SIM	ABERTO E FECHADO
Critério de Julgamento			
MENOR PREÇO GLOBAL		SIGILOSO, NOS TERMOS DO ART. 24 DA LEI Nº 14.133 DE 2021	
Lic. Exclusiva ME/EPP?		Exige Amostra / Dem.?	
NÃO		NÃO	
Prazo para envio da proposta/documentação			
Até às 09h30min do dia 07/05/2026 (data e horário estabelecidos para abertura da sessão pública)			
Pedidos de Esclarecimentos			
Até o dia 04/05/2026 para o endereço licitacoes@mpmt.mp.br (até 03 dias úteis anteriores à data fixada para abertura da sessão pública)			
Impugnações			
Até o dia 04/05/2026 para o endereço licitacoes@mpmt.mp.br (até 03 dias úteis anteriores à data fixada para abertura da sessão pública)			
Observações Gerais			
A FALSIDADE DA DECLARAÇÃO QUANTO ÀS CONDIÇÕES DE PARTICIPAÇÃO, REFERENTE AO ENQUADRAMENTO COMO ME/EPP, SUJEITARÁ A LICITANTE ÀS SANÇÕES PREVISTAS NA LEI Nº 14.133, DE 2021 E NESTE EDITAL.			





Pregão Eletrônico n. 18/2026 do Tribunal Regional Eleitoral do Estado de São Paulo



TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO

TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE SÃO PAULO				
Pregão Eletrônico Federal n.º 90018/2026				
Regido pela Lei n.º 14.133, de 1º de abril de 2021, pela IN SEGES/ME nº 73, de 30 de setembro de 2022, pelo Decreto nº 11.462, de 31 de março de 2023, pela Lei Complementar n.º 123, de 14 de dezembro de 2006 e alterações posteriores, regulamentada pelo Decreto n.º 8.538, de 6 de outubro de 2015, bem como pela Lei n.º 8.078 de 11 de setembro de 1990 e demais legislações aplicáveis, e, ainda, de acordo com as condições estabelecidas no Edital, Anexos e Apêndices.				
Objeto: Registro de preços para emissão de certificados digitais dentro das especificações e normas ICP-Brasil, para pessoa física e jurídica, incluindo o fornecimento de dispositivos criptográficos <i>TOKENS USB</i> para armazenamento.				
Observação: Havendo divergência entre a descrição do(s) item(ns) e o código/descrição do CATMAT/CATSER prevalecerão as especificações detalhadas no Anexo I (Termo de Referência) deste Edital.				
Data de abertura da sessão pública: 12/06/2026 às 13h no site www.gov.br/compras/pt-br				
Registro de Preços? (x) Sim () Não	Tipo: Menor preço	Modo de disputa: Aberto	Edital exclusivo ME/EPP? () Sim (x) Não	Edital híbrido? () sim (x) não
Processo SEI: 0018912-98.2025.6.26.8000			Reserva de cota ME/EPP? () Sim (x) Não	Qual(is) item(ns) exclusivo(s) ME/EPP: não se aplica
Valor total estimado: R\$ 141.590,02			Apresentação de amostra? () Sim (x) Não	Vistoria prévia? () Obrigatória; () Facultativa; (x) não se aplica
Critério de Julgamento: Menor preço global do grupo único			Apresentação de prova? () Sim (x) Não	
Quantidade de itens: 2 itens			Quantidade de grupos: grupo único	
Licitação Sustentável? () Sim (x) Não Indicação do critério de sustentabilidade: não se aplica				
Pedidos de esclarecimentos e impugnações: Até às 23h59 de 09/06/2026. Os pedidos de esclarecimentos e as impugnações referentes a este procedimento devem ser encaminhados exclusivamente por meio eletrônico via internet, para o endereço pregoeiro@tre-sp.jus.br				
Documentos de habilitação:				
Cláusula 15 do Edital				

Endereço da Seção de Elaboração de Editais e Contratos: Rua Francisca Miquelina, 123, Prédio Brigadeiro, 11º andar, sala 1101, Bela Vista, São Paulo CEP: 01316-900.

Retire o Edital e acompanhe esta licitação e seus atos na internet pelos portais <http://www.tre-sp.jus.br/transparencia-e-prestacao-de-contas/licitacoes/licitacoes> e www.gov.br/compras/pt-br





ANEXO C – REQUISITOS TÉCNICOS

Item 1. Serviço de Validação e Emissão de Certificado Digital – Cert-JUS A3 (Pessoa Física) – Validade 24 meses – SEM Mídia Criptográfica (Nuvem).

Padrão Técnico do Certificado Digital A3 em Nuvem:

A solução de certificação digital A3 em nuvem deverá atender integralmente às normas da ICP-Brasil, às diretrizes do Conselho Nacional de Justiça e aos princípios da Lei Geral de Proteção de Dados Pessoais – LGPD, assegurando autenticação forte, custódia segura das chaves criptográficas, rastreabilidade das operações, possibilidade de revogação ou bloqueio em caso de incidente e governança sobre o uso do certificado, com nível de segurança equivalente ou superior ao certificado A3.

A solução deverá observar, no mínimo, os seguintes requisitos técnicos:

- As chaves privadas deverão ser geradas e armazenadas em ambientes criptográficos seguros, não sendo exportáveis nem armazenadas no computador do usuário.
 - Os HSMS utilizados para custódia e operação das chaves criptográficas deverão possuir certificação mínima FIPS 140-2 ou superior, contemplando:
 - proteção física contra violação;
 - mecanismos de detecção e resposta a tentativas de acesso indevido;
 - armazenamento seguro de chaves criptográficas;
 - controle de acesso lógico e físico ao ambiente criptográfico.
 - Deverão ser utilizados algoritmos criptográficos homologados e vigentes no âmbito da ICP-Brasil, contemplando, no mínimo:
 - chaves criptográficas RSA de 2048 bits ou superior, ou padrão equivalente homologado pela ICP-Brasil;
 - funções de resumo criptográfico SHA-256 ou superior;
 - algoritmos de assinatura digital compatíveis com os padrões da ICP-Brasil, tais como sha256WithRSAEncryption, sha512WithRSAEncryption ou equivalentes homologados.
 - O acesso à chave privada deverá ser mediado por mecanismos criptográficos, controles de autorização e políticas de segurança aplicáveis ao uso do certificado digital.
- A Autoridade Certificadora, Autoridade Provedora do Certificado, Prestador de Serviço de Confiança ou entidade responsável pela solução deverá disponibilizar, quando aplicável, ao menos uma das seguintes formas de integração:
- via PKCS#11, por meio de biblioteca compatível e configurável; ou
 - via MSCAPI/CSP, utilizando integração nativa do Windows, configurável no





assinador em modo “Windows”; ou

- outro mecanismo tecnicamente equivalente, homologado e compatível com os sistemas utilizados pela CONTRATANTE.
 - A integração deverá preservar a segurança da chave privada, sendo vedada sua exportação, cópia ou armazenamento local no computador do usuário, mantendo a custódia em ambiente criptográfico seguro e homologado.
 - O uso do certificado deverá exigir autenticação forte e multifator, por meio da combinação de fatores de autenticação, tais como:
 - senha ou PIN do certificado;
 - dispositivo previamente autorizado, como computador, celular ou aplicativo autenticador;
 - biometria facial, biometria digital, token lógico, aplicativo seguro ou outro mecanismo equivalente de autenticação forte.
 - O acesso e a utilização da chave privada associada ao certificado digital em nuvem deverão ser protegidos por mecanismo de autenticação pessoal e intransferível, definido pelo titular, observadas as diretrizes da ICP-Brasil e as boas práticas de
 - A solução deverá possuir mecanismo de bloqueio temporário ou permanente após sucessivas tentativas inválidas de autenticação, de modo a prevenir o acesso e a utilização não autorizados do certificado digital.
 - Toda comunicação realizada entre o usuário, o aplicativo, a plataforma de assinatura, a infraestrutura de certificação e os mecanismos de auditoria deverá ocorrer por canais criptografados, utilizando TLS 1.2 ou superior, ou protocolo equivalente homologado e vigente.
 - Por se tratar de certificado A3 em nuvem, não deverá haver necessidade de recolhimento físico de mídia criptográfica, reduzindo o tempo de resposta em situações de bloqueio, suspensão, revogação ou substituição do certificado.
- A solução deverá possuir aderência integral às:
- normas, políticas e diretrizes da ICP-Brasil;
 - exigência de credenciamento do fornecedor como Prestador de Serviço de Confiança – PSC, nos termos do DOC-ICP-17, quando aplicável;
 - políticas da cadeia Cert-JUS;
 - resoluções e diretrizes do Conselho Nacional de Justiça;
- princípios da LGPD, especialmente segurança, prevenção, responsabilização, prestação de contas, confidencialidade, integridade e minimização de riscos.

Redefinição de Senha pelo Usuário:





Deverá permitir a redefinição de senha nos casos de bloqueio, esquecimento ou sempre que o usuário desejar realizar a alteração de sua credencial de acesso.

O processo de redefinição de senha deve ser simples, seguro e intuitivo, onde apenas o titular do certificado possa realizar a alteração, utilizando métodos de autenticação robustos, tais como, mas não se limitando:

- Perguntas de segurança, biometria ou autenticação multifatorial (MFA); ou
- Confirmação via e-mail funcional ou SMS, ou gestão pelo software homologado (sujeito a testes de usabilidade).

Gestão e Compartilhamento Seguro do Certificado em Nuvem:

O certificado digital, por estar armazenado em nuvem, deve possibilitar compartilhamento seguro através de aplicativo dedicado. O titular deve manter controle total sobre:

- autorizações concedidas;
- dispositivos autorizados;
- Revogação de acesso;
- acessos realizados;
- Todas as assinaturas devem ser autorizadas.

Revogação de Acessos:

A solução deverá permitir o gerenciamento de acessos de terceiros ao certificado digital, possibilitando a concessão, restrição e revogação imediata das permissões, sem necessidade de emissão de novo certificado.

O titular deve poder configurar o período de validade do compartilhamento e definir permissões temporárias para cada dispositivo ou usuário autorizado.

Um mesmo certificado em nuvem deve poder ser utilizado em múltiplos sistemas e aplicações, sem que isso represente contagem ou emissão de certificados adicionais.

A solução deverá permitir resposta tempestiva a incidentes de segurança, contemplando:

- revogação imediata do certificado, quando aplicável;
- bloqueio instantâneo;
- suspensão temporária do uso do certificado;
- registro e rastreabilidade das ações realizadas.

Autorização para Uso em Desktops:

Para utilização do certificado digital em computadores institucionais ou pessoais, a solução deverá exigir autorização prévia, explícita e individual do titular do certificado, garantindo o controle sobre os dispositivos habilitados para uso.

A solução deve registrar e disponibilizar informações de rastreabilidade, permitindo verificar:

- dispositivos autorizados;
- data e hora de acesso;
- histórico de uso;
- permissões concedidas ou revogadas.





A solução deverá permitir a gestão dos dispositivos e acessos autorizados, contemplando:

- autorização e revogação de dispositivos;
- limitação de períodos de uso;
- definição de permissões temporárias;
- bloqueio ou suspensão de acesso em caso de suspeita de uso indevido.

Disponibilizar drivers e bibliotecas compatíveis com os sistemas operacionais Windows 10 e Windows 11 (arquiteturas x64 e x86, ou superior quando aplicável) e macOS (versões suportadas pelo fabricante).

Item 2. Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3 com Validade de 24 meses para Pessoa Física COM Fornecimento de Mídia Criptográfica (Token USB).

Padrão Técnico da Mídia Criptográfica:

A solução de certificação digital A3 token físico deverá atender integralmente às normas da ICP-Brasil, às diretrizes do Conselho Nacional de Justiça e aos princípios da Lei Geral de Proteção de Dados Pessoais – LGPD, assegurando autenticação forte, custódia segura das chaves criptográficas, rastreabilidade das operações, possibilidade de revogação ou bloqueio em caso de incidente e governança sobre o uso do certificado, com nível de segurança equivalente ou superior ao certificado A3.

O certificado digital do tipo A3 em mídia criptográfica física deverá adotar mecanismos de segurança física e lógica, assegurando que as chaves criptográficas privadas sejam geradas e armazenadas exclusivamente no dispositivo criptográfico, em memória segura, não exportável e protegida por senha ou PIN pessoal do titular.

A mídia fornecida deverá atender integralmente aos padrões técnicos da ICP-Brasil, possuir certificação mínima FIPS 140-2 ou superior, oferecer compatibilidade com os sistemas operacionais Windows 10, Windows 11 e macOS, bem como assegurar a integridade, confidencialidade, autenticidade e validade jurídica das assinaturas realizadas.

A mídia fornecida, no formato token USB, deverá observar, no mínimo, os seguintes requisitos técnicos:

- As chaves criptográficas privadas deverão ser:
 - geradas dentro do próprio token;
 - armazenadas em memória criptográfica segura interna;
 - inacessíveis ao sistema operacional para fins de cópia, extração ou exportação;
 - vinculadas exclusivamente ao dispositivo criptográfico fornecido.
- Deverão ser utilizados algoritmos criptográficos homologados e vigentes no âmbito da ICP-Brasil, contemplando, no mínimo:





- chaves criptográficas RSA de 2048 bits ou superior, ou padrão equivalente homologado pela ICP-Brasil;
 - funções de resumo criptográfico SHA-256 ou superior;
 - algoritmos de assinatura digital compatíveis com os padrões da ICP-Brasil, tais como sha256WithRSAEncryption, sha512WithRSAEncryption ou equivalentes homologados.
- A mídia criptográfica deverá atender integralmente aos padrões técnicos da ICP-Brasil aplicáveis aos dispositivos A3 em mídia física.
- A chave privada deverá permanecer protegida mesmo em caso de acesso físico ao dispositivo, sendo vedada sua extração, cópia, exportação ou armazenamento no computador do usuário.
- A chave privada deverá:
- nunca ser exportável;
 - não permitir cópia para o computador do usuário ou para qualquer outro dispositivo;
 - permanecer vinculada exclusivamente ao token USB;
 - ser utilizada apenas mediante autenticação do titular.
- A mídia criptográfica deverá possuir memória criptográfica segura compatível com a finalidade do certificado digital A3, suficiente para:
- armazenamento das chaves criptográficas;
 - armazenamento dos certificados digitais;
 - funcionamento adequado das operações de autenticação e assinatura digital.
- O acesso ao certificado deverá exigir:
- senha ou PIN pessoal, definido pelo titular;
 - A mídia deverá possuir política de bloqueio automático após tentativas inválidas consecutivas de autenticação, prevenindo o uso indevido do certificado em caso de tentativa de acesso não autorizado.
 - A proteção do certificado armazenado na mídia criptográfica deverá ser realizada por senha ou PIN pessoal, definido pelo titular, observadas as diretrizes da ICP-Brasil e as boas práticas de segurança aplicáveis.
- A solução deverá permitir:
- alteração de senha ou PIN pelo usuário, quando aplicável;
 - desbloqueio, substituição ou reemissão mediante procedimento seguro junto à Autoridade de Registro — AR ou Autoridade Certificadora responsável;
 - revogação do certificado em caso de perda, roubo, extravio, comprometimento da senha ou suspeita de uso indevido mediante solicitação formal do titular ou da Administração, quando cabível.
- Deverão ser disponibilizados:
- drivers e bibliotecas oficiais do fabricante;





- manuais ou orientações técnicas de instalação e utilização;
 - suporte à configuração do token nos ambientes compatíveis;
 - atualização dos componentes necessários ao funcionamento seguro da mídia criptográfica.
- A mídia criptográfica deverá possuir compatibilidade com:
- assinadores e aplicações utilizados pelo Poder Judiciário que demandem certificado digital A3;
 - sistemas e plataformas que utilizem certificados digitais emitidos no âmbito da ICP-Brasil.
 - Os drivers, bibliotecas e componentes de software necessários ao funcionamento da mídia deverão:
 - ser oficiais do fabricante;
 - não exigir hardware adicional além do próprio token USB;
 - manter compatibilidade com assinadores e aplicações que utilizem certificados digitais ICP-Brasil;
- A Autoridade Certificadora, Autoridade Provedora do Certificado, Prestador de Serviço de Confiança ou entidade responsável pela solução deverá disponibilizar, quando aplicável, ao menos uma das seguintes formas de integração:
- via PKCS#11, por meio de biblioteca compatível e configurável; ou
 - via MSCAPI/CSP, utilizando integração nativa do Windows, configurável no assinador em modo “Windows”; ou
 - outro mecanismo tecnicamente equivalente, homologado e compatível com os sistemas utilizados pela CONTRATANTE.
- Em caso de perda, roubo, extravio, comprometimento da senha/PIN, suspeita de uso indevido ou violação da mídia criptográfica, o certificado deverá ser formalmente revogado junto à Autoridade Certificadora responsável, observando os procedimentos definidos pela ICP-Brasil e pela cadeia de certificação aplicável.
- A utilização da mídia criptográfica física deverá observar integral aderência às:
- normas, políticas e diretrizes da ICP-Brasil;
 - políticas da cadeia Cert-JUS, quando aplicável;
 - resoluções e diretrizes do Conselho Nacional de Justiça;
- princípios da LGPD, especialmente segurança, prevenção, responsabilização, prestação de contas, confidencialidade, integridade e minimização de riscos.

Envio do Certificado Digital físico:

A CONTRATADA será responsável pelo envio das mídias criptográficas, tais como tokens USB, às unidades indicadas pela CONTRATANTE, conforme relação constante no Anexo XX.

A entrega deverá ser realizada exclusivamente por meio de SEDEX ou serviço equivalente de encomenda expressa, com prazo compatível para o recebimento dos dispositivos físicos na comarca ou unidade de lotação do solicitante.





O envio deverá ser realizado em nome do solicitante, direcionado à comarca ou unidade indicada pela CONTRATANTE, observando os procedimentos de rastreabilidade, segurança e controle de entrega.

A CONTRATADA deverá apresentar o protocolo de envio, contendo obrigatoriamente o respectivo código de rastreamento, no prazo máximo de 8 horas úteis após a abertura do ticket, tendo seu envio registrado no ticket para acompanhamento da fiscalização. O descumprimento desse prazo poderá ensejar a aplicação das penalidades previstas nos indicadores e níveis de serviço estabelecidos no contrato.

Para o envio dos certificados em mídia física, deverá ficar expressamente estabelecido que a CONTRATADA será integralmente responsável pela logística de remessa dos dispositivos, sendo vedada qualquer cobrança adicional ao Tribunal.

O envio deverá ser realizado diretamente ao gestor, responsável administrativo ou solicitante da comarca ou unidade indicada, na condição de responsável pelo recebimento institucional. Após o devido registro interno, caberá ao responsável pelo recebimento efetuar a entrega do token em mãos ao solicitante final, garantindo a rastreabilidade do dispositivo, a adequada guarda e o controle até sua efetiva disponibilização.

Para conclusão do processo de emissão do certificado digital físico, a CONTRATADA deverá manter controle formal da entrega do token ao solicitante final, registrando a confirmação de recebimento e vinculando-a ao respectivo pedido, voucher, carta de autorização ou ticket correspondente. A emissão do certificado somente deverá ser concluída após a confirmação da entrega da mídia criptográfica ao solicitante, de modo a assegurar a rastreabilidade integral do processo.

Item 3. Pontos de Atendimento Presencial e Visita Técnica para Emissão

A CONTRATADA deverá prever a disponibilização de dois pontos de atendimento de apoio, sendo um localizado no município de Cuiabá/MT e outro no município de Várzea Grande/MT, com estrutura adequada para prestar a emissão, validação, ativação e uso do certificado digital seja físico ou em nuvem.

A CONTRATADA deverá prever que a emissão do voucher e da respectiva carta de autorização/carta de serviço ocorra conforme o fluxo definido pela CONTRATANTE, observando o agendamento prévio. Somente poderão avançar para a etapa de emissão e validação os usuários previamente autorizados pela CONTRATANTE, mediante apresentação do voucher e da carta de autorização.

O atendimento deverá observar as seguintes condições:

- Disponibilização de ponto de atendimento em Cuiabá/MT;
- Disponibilização de ponto de atendimento em Várzea Grande/MT;
- Emissão ou controle do voucher vinculado ao solicitante autorizado;
- Vinculação do atendimento à respectiva carta de autorização/carta de serviço emitida pela CONTRATANTE;





- Registro do atendimento na ferramenta da CONTRATANTE, contendo data, horário, nome do solicitante, matrícula, e-mail funcional, número do voucher, responsável pelo atendimento e situação do processo;

Sobre as visitas técnicas presenciais; quando solicitadas, deverão ser previamente avaliadas pela Fiscalização do Contrato e somente poderão ocorrer após autorização formal do fiscal, mediante emissão da respectiva Carta de Autorização de Visita.

Após autorização formal da Fiscalização do Contrato, a CONTRATADA deverá realizar o agendamento da visita técnica com a unidade ou usuário responsável e executar a visita no prazo máximo de 2 dias úteis, contados da autorização formal, salvo nos casos em que houver necessidade de reagendamento por indisponibilidade do usuário, da unidade ou por motivo devidamente justificado e registrado no respectivo ticket.

As visitas deverão ser realizadas exclusivamente nos municípios de Cuiabá/MT e Várzea Grande/MT, com a finalidade específica de viabilizar a emissão, validação, ativação ou suporte relacionado aos certificados digitais contratados.

Cuiabá/MT

- TJMT - Poder Judiciário do Estado de Mato Grosso - Centro Político Administrativo - Rua C, S/N - CEP 78049-926 - Cuiabá-MT - (65) 3617-3000;
- Fórum de Cuiabá - Av. Des. Milton Figueiredo Ferreira Mendes, s/nº - Centro Político Administrativo - Cuiabá - MT - 78049-075
- Complexo dos Juizados Especiais de Cuiabá - R. Dr Helio Ponce De Arruda, 857 - Centro Político Administrativo, Cuiabá - MT, 78050-911

Várzea Grande/MT

- Fórum de Várzea Grande - Av. Chapéu do Sol - Guarita II, Várzea Grande - MT, 78158-720

A solicitação de visita técnica deverá ser formalizada junto à Fiscalização do Contrato, por meio da ferramenta oficial de gestão de atendimentos da CONTRATANTE, contendo as informações necessárias para análise e autorização prévia.

Toda visita técnica autorizada deverá ser obrigatoriamente registrada no sistema da CONTRATANTE, contendo as seguintes informações:

- nome do solicitante e/ou usuário atendido;
- data e horário;
- local de realização da visita;
- número do ticket ou solicitação vinculada;
- número do voucher;





- responsável pela execução da visita;
- finalidade do atendimento;
- anexo da Carta de Autorização de Visita, devidamente assinada pelo fiscal do contrato.

A realização da visita técnica não dispensa a observância dos procedimentos de segurança, rastreabilidade, validação de identidade, conformidade com a ICP-Brasil, cadeia Cert-JUS e demais normativos aplicáveis à emissão de certificados digitais.

A CONTRATADA deverá assegurar a rastreabilidade integral das visitas técnicas, mantendo os registros atualizados no sistema, de modo a permitir o acompanhamento pela Fiscalização e a adequada gestão do serviço.

O fluxo mínimo para realização da visita técnica presencial deverá observar a seguinte sequência:

- Abertura da solicitação na ferramenta oficial da CONTRATANTE;
- Análise da necessidade pela Fiscalização do Contrato;
- Emissão da Carta de Autorização de Visita, quando aprovada;
- Agendamento da visita pela CONTRATADA com a unidade ou usuário responsável;
- Execução da visita no prazo máximo de 2 dias úteis após a autorização formal;
- Registro da execução no ticket correspondente;
- Anexação das evidências e da Carta de Autorização de Visita;
- Atualização da situação do atendimento;
- Encerramento do ticket após validação das informações registradas.





ANEXO D – ORÇAMENTOS

Os valores unitários e total referentes à toda solução constam da tabela abaixo.





Registro de Preços para Certificados Digitais Cert-JUS A3 - 24 meses														
LOTE	Item	Descrição	Tipo	Qtd	PREÇOS PRIVADOS			PREÇO PÚBLICO		Valor Unitário Média	Valor Unitário Mediana	Valor Total Média	Valor Total Mediana	
					Xdigital Brasil	AR RP Certificação	Certisign	Valid	Contrato n. 128/2024 TJMT					Contrato n. 13/2024 MTI
Lote Único	1	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, em nuvem, com validade de 24 meses (e-CPF) para pessoa física (e-CPF), sem fornecimento de mídia criptográfica.	Serviço	4000	R\$ 530,00	R\$ 660,00	R\$ 183,99	R\$ 208,00	-	-	R\$ 395,50	R\$ 369,00	R\$ 1.582.000,00	R\$ 1.476.000,00
	2	Serviço de Validação e Emissão de Certificado Digital Cert-JUS A3, com validade de 24 meses (e-CPF) para pessoa física com o fornecimento do token.	Serviço	7000	R\$ 420,00	R\$ 790,00	R\$ 282,99	R\$ 395,00	-	-	R\$ 472,00	R\$ 407,50	R\$ 3.304.000,00	R\$ 2.852.500,00
	3	Serviço de Visita Técnica para Emissão de Certificados Digitais	Serviço	150	R\$ 450,00	R\$ 300,00	R\$ 1.859,00	R\$ 250,00	R\$ 20,00	R\$ 37,00	R\$ 486,00	R\$ 275,00	R\$ 72.900,00	R\$ 41.250,00
	TOTAL										R\$ 1.353,50	R\$ 1.051,50	R\$ 4.958.900,00	R\$ 4.369.750,00
TOTAL DA ATA DE REGISTRO DE PREÇOS PARA 24 MESES												R\$ 4.369.750,00		





RADAR ELETRÔNICO TCE / MT: Em pesquisa realizada no Radar Eletrônico do Tribunal de Contas do Estado de Mato Grosso, considerando o objeto e as especificações relacionadas à emissão de certificados digitais e ao fornecimento de mídias criptográficas, não foram identificados registros de contratações recentes com objeto e especificações suficientemente similares que pudessem ser utilizados como referência direta para a presente contratação, conforme relatório de pesquisa anexo.

CATÁLOGO DE PREÇOS DA SECRETARIA DE GOVERNO DIGITAL: Em atendimento ao artigo 8º da Instrução Normativa SEGES/ME nº 65/2021, foi realizada pesquisa no *Catálogo de Soluções de TIC com Condições Padronizadas*, disponível no endereço eletrônico: <https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/catalogo-de-produtos-e-servicos-microsoft-versao-4-0-0.pdf>.

O resultado da pesquisa foi o seguinte: O objeto que será contratado não está composto no referido catálogo.

PREÇOS PÚBLICOS: Art 5º, inc. I e II, IN SEGES/ME nº 65/2021: Foram realizadas pesquisas em bases de preços públicos, incluindo o Pannel de Preços do Governo Federal, o Portal Nacional de Contratações Públicas (PNCP), o Banco de Preços e sites oficiais de órgãos públicos, buscando identificar contratações similares que pudessem ser utilizadas como referência para a estimativa de preços.

Não foram identificadas contratações públicas que apresentassem, simultaneamente, as mesmas especificações, quantitativos similares e vigência de 24 (vinte e quatro) meses previstas para a presente contratação.

Para o Item 3 – Serviço de Visita Técnica para Emissão de Certificados Digitais, entretanto, foram identificadas referências de preços em contratações realizadas no âmbito do Estado de Mato Grosso, consideradas mais aderentes à realidade da presente contratação, especialmente o Contrato nº 128/2024/TJMT e o Contrato nº 13/2024/MTI.

Assim, para esse item, foram utilizados os valores constantes das referidas contratações como referências de preços públicos, por se tratarem de contratações realizadas por órgãos públicos do Estado de Mato Grosso e apresentarem maior equivalência com as características do serviço pretendido pelo TJMT.

ORÇAMENTOS: No tocante ao Art 5º, inc. IV, IN SEGES/ME nº 65/2021: Complementarmente, mediante solicitação de cotações diretamente a empresas atuantes no mercado de certificação digital e credenciadas no âmbito da ICP-Brasil, aptas a fornecer os serviços objeto da contratação.

Foram obtidas propostas das empresas Xdigital Brasil, AR RP Certificação, Certisign e Valid, contemplando os serviços de validação e emissão de certificados digitais Cert-JUS A3 em nuvem e com fornecimento de token, bem como o serviço de visita técnica para emissão dos certificados.

METODOLOGIA MATEMÁTICA ADOTADA E JUSTIFICATIVA: Art. 3º, inciso VI e art. 6º, caput, §2º e §3º IN SEGES /ME Nº 65/2021º:

a definição do valor estimado da contratação foi realizada mediante análise dos preços obtidos nas pesquisas de mercado público e privado, considerando-se, para cada item, os valores unitários identificados nas fontes consultadas.

Para a composição da estimativa, foram calculadas a média e a mediana dos preços válidos obtidos para cada item, sendo adotada a mediana como parâmetro para definição do valor estimado da contratação, por apresentar menor sensibilidade a eventuais valores discrepantes e proporcionar maior representatividade dos preços praticados no mercado.

Com base nessa metodologia, o valor estimado para a Ata de Registro de Preços, considerando os quantitativos previstos e a vigência de 24 (vinte e quatro) meses, corresponde a R\$ 4.369.750,00, conforme demonstrado na planilha de estimativa de preços.





RADAR APLIC TCE

Em pesquisa no Radar Eletrônico do Tribunal de Contas do Estado de Mato Grosso, não foram encontrados resultados relacionados ao assunto da licitação ou aos itens que a compõem.

											
Relatório Resumido											
Relatório gerado em: 25/08/2026 08:58:33 Quantidade total de registros: 2											
Filtros aplicados											
Objeto da licitação: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA EMISSÃO DE CERTIFICADO DIGITAL A3 CPF E CNPJ SEM MEDIA PARA 2 ANOS Tipo de Licitação: Não contempla/não favorece Para Registro de Preços: Não informado											
Valor Máximo Unit do Material				Média Saneada Global				Mediana Valor Unit do Material			
R\$235,00				R\$1018507,50				R\$202,50			
Fiscalizado	Modalidade	Cód. Licitação	Cód. Material	Material	Descrição	Quantidade	Unid. Fornecimento	Valor Unit	CNPJ/CPF Fornecedor	Nome Fornecedor	Data Homologação
CM DE VILA BELA DA SANTISSIMA TRINDADE	Dispensa de licitação	00000000002/2019	336832-7	SERVICO DE ASSINATURA DE JORNAIS E PERIODICOS	(336832-7) SERVICO DE ASSINATURA DE JORNAIS E PERL.	1	UNIDADE	R\$ 170,00	29.063.876/0001-69	CERTIFICA CERTIFICACAO DIGITAL LTDA	14/02/2019
CM DE VILA BELA DA SANTISSIMA TRINDADE	Dispensa de licitação	00000000002/2019	434099-0	SERVICO DE ACESSO E UTILIZACAO	(434099-0) SERVICO DE ACESSO E UTILIZACAO - EMISSA.	1	UNIDADE	R\$ 235,00	29.063.876/0001-69	CERTIFICA CERTIFICACAO DIGITAL LTDA	14/02/2019

Em consulta ao Radar do Tribunal de Contas do Estado de Mato Grosso, foi localizada contratação com objeto relacionado à emissão de certificados digitais, conforme relatório de pesquisa.

Entretanto, a referência identificada não foi considerada para composição da estimativa de preços, tendo em vista que a contratação foi realizada em 2019, portanto não representa condição de mercado atual, e ocorreu por meio de dispensa de licitação, não sendo compatível com a metodologia adotada para a presente pesquisa de preços.





Protocolo de Assinatura(s)

O documento acima foi assinado eletronicamente, na plataforma de assinaturas do Poder Judiciário do Estado de Mato Grosso.

Para assegurar a autenticidade e validar as assinaturas, utilize o endereço abaixo.

<https://validador.tjmt.jus.br/codigo/AD:15B60000-0AA6-0A58-0085-08DF02D4117B>

Código verificador - AD:15B60000-0AA6-0A58-0085-08DF02D4117B



**THIAGO APOLONIO DE
ASSUNCAO SILVA**

Assinado em 25/08/2026 14:09:56



**JEFFERSON DE MATTOS
DOMINGOS**

Assinado em 25/08/2026 14:11:14



**MARCOS PINTO GOMES
JUNIOR**

Assinado em 25/08/2026 15:02:11



ÂNGELA MARIA FRANCHINI

Assinado em 25/08/2026 15:17:01



**FABIO CARLOS ARRUDA DA
SILVA**

Assinado em 25/08/2026 15:29:40



**MOACYR JOSE COUTO DAIMA
FILHO**

Assinado em 25/08/2026 18:25:49



**MARCIA REGINA DE
CARVALHO BUHR**

Assinado em 25/08/2026 19:52:02