



TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO

ESTUDOS TÉCNICOS Nº 989

1. INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

O Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial), instituído pelo Decreto nº 8.373/2014, é hoje uma realidade consolidada para todos os empregadores no Brasil. O sistema transformou a maneira como as empresas se comunicam com o Governo, unificando o envio de informações cruciais sobre seus trabalhadores.

Por meio do eSocial, informações como vínculos empregatícios, contribuições previdenciárias, folhas de pagamento, comunicações de acidente de trabalho, avisos prévios, escriturações fiscais e dados sobre o FGTS são transmitidas de forma eletrônica e padronizada. Esta abordagem digital simplificou significativamente a prestação de contas, reduzindo a burocracia ao substituir o preenchimento e a entrega de múltiplos formulários e declarações a diferentes entes governamentais.

A implementação do eSocial, que ocorreu em fases ao longo dos últimos anos, já está completa, incluindo a quarta fase, que tornou obrigatório o envio dos eventos de Saúde e Segurança do Trabalho (SST). O sistema continua em constante aprimoramento, com novas versões e atualizações sendo disponibilizadas para melhorar a qualidade e a segurança das informações. Para 2025, por exemplo, está prevista a substituição definitiva da Declaração do Imposto de Renda Retido na Fonte (DIRF) pelas informações prestadas através do eSocial.

Os principais objetivos do sistema permanecem os mesmos: garantir os direitos previdenciários e trabalhistas, racionalizar e simplificar o cumprimento das obrigações, eliminar a redundância de informações e aprimorar a qualidade dos dados sobre as relações de trabalho, previdenciárias e tributárias.

Para a transmissão dos dados ao eSocial, é exigido o uso de certificado digital, sendo o e-CNPJ (para pessoas jurídicas) o padrão utilizado, garantindo a autenticidade e a segurança das informações enviadas.

Neste cenário de intensa digitalização, a segurança da informação é primordial. Além dos certificados para a transmissão de dados, as empresas/órgãos gerenciam diversos portais e sistemas online (como portais do cliente, áreas de acesso restrito, etc.). Para proteger a comunicação nestas plataformas, é fundamental a utilização de um **certificado SSL Wildcard**. Este tipo de certificado permite proteger o domínio principal de um site e um número ilimitado de subdomínios (ex: portal.suaempresa.com.br, clientes.suaempresa.com.br, etc.) com uma única instalação. A importância de sua utilização reside na capacidade de criptografar os dados trocados entre o usuário e o servidor, garantindo a confidencialidade e a integridade das informações e fortalecendo a confiança do cliente na segurança da empresa/órgão.

É importante destacar que, em um contexto distinto, os certificados digitais do tipo e-CPF são de uso pessoal e comumente utilizados por servidores públicos para acessar sistemas como o Processo Judicial Eletrônico (PJe) e o portal Gov.br. Estes certificados possuem validade determinada e a demanda por sua emissão e renovação é uma constante na administração pública.

1.1. Definição e Especificação dos Requisitos da Demanda

a) Especificação Técnica - Certificado Tipo A1 (e-CNPJ)

1. Autoridade Certificadora

- Deve ser emitido por **Autoridade Certificadora (AC) credenciada pela Infraestrutura de Chaves Públicas Brasileira ICP-Brasil**.

2. Padrões de Assinatura Digital

- Deve permitir o uso do padrão de assinatura digital XML Digital Signature, no modo Enveloped, conforme normas da ICO-Brasil;
- O certificado deve estar em conformidade com certificado digital X.509 versão 3;
- A chave de criptografia deve ter o tamanho mínimo de **2048 bits RSA** (ou superior), conforme requisitos da ICP-Brasil;
- O algoritmo de resumo de mensagem deve ser **SHA-256**;
- Deve suportar as transformações **Enveloped** e **C14N (Canonical XML)**;
- O certificado deve permitir também uso em padrões de assinatura **PCKS#7 / CMS**, quando aplicável (ex.: PDF).

3. Validação da Assinatura

- Deve permitir a validação de assinatura digital, garantindo:
 - **Integridade** do documento;
 - **Autoria** do signatário;
 - **Validade da cadeia de certificação**, incluindo a verificação das **Listas de Certificados Revogados (LCR/CRL)** ou equivalente (OCSP).

4. Conformidade Normativa

- Deve ser plenamente aderente às normas e diretrizes técnicas do **Comitê Gestor da ICP-Brasil**.

5. Compatibilidade

- Deve ser compatível com sistemas operacionais **Linux** e **Windows**;
- O certificado deve ser fornecido em formato **PKCS#12 (.pfx ou .p12)**, contendo chave privada e cadeia de certificação.

6. Validade

- O certificado digital deve possuir validade de **1 (um) ano**;

b) Especificação Técnica - Certificado Tipo A3 (e-CPF) em Nuvem

1. Autoridade Certificadora

- Deve ser emitido por **Autoridade Certificadora (AC) credenciada pela Infraestrutura de Chaves Públicas Brasileira ICP-Brasil**.

2. Tipo e Armazenamento

- O certificado deve ser do tipo A3, emitido e armazenado em **ambiente seguro em nuvem** (HSM - Hardware Security Module ou equivalente certificado);
- A chave privada deve ser **gerada e mantida exclusivamente em módulo criptográfico seguro** em conformidade com a ICP-Brasil, sem possibilidade de exportação pelo titular.

3. Padrões de Assinatura Digital

- O certificado deve estar em conformidade com o padrão **X.509 versão 3**;
- A chave criptográfica deve ter tamanho mínimo de **2048 bits RSA** (ou superior), conforme requisitos da ICP-Brasil;
- O algoritmo de resumo de mensagem deve ser **SHA-256**;
- Deve suportar padrões de assinatura **XML Digital Signature** (Enveloped e Canonical XML - C14N) e **PKCS#7 / CMS** (assinatura de PDF e outros documentos).

4. Validação da Assinatura

- Deve permitir a validação da assinatura digital, garantindo:
 - **Integridade** do documento;
 - **Autoria** do signatário
 - **Validade da cadeia de certificação**, incluindo a verificação das **Listas de Certificados Revogados (LCR/CRL)** ou equivalente (OCSP).

5. Conformidade Normativa

- Deve ser plenamente aderente às normas e diretrizes técnicas do **Comitê Gestor da ICP-Brasil**, incluindo as resoluções específicas para certificados em nuvem.

6. Compatibilidade e Acesso

- O acesso ao certificado deve ser possível por meio de **aplicativo (desktop, web ou mobile)** disponibilizado pela AC, garantindo integração com sistemas operacionais Windows, Linux e Android/iOS, conforme aplicável;
- O uso do certificado deve requerer **autenticação multifator** (senha/PIN + segundo fator, como OTP, biometria ou push notification).

7. Validade

- O certificado digital deve possuir validade de **até (cinco) anos**, conforme normas ICP-Brasil para certificados A3 em nuvem.

c) Especificação Técnica - Certificado SSL/TLS Wildcard OV (Organizational Validation)

1. Autoridade Certificadora

- O certificado deve ser emitido por **Autoridade Certificadora (CA) internacional reconhecida mundialmente**, integrante da lista de **Root Programs de navegadores e sistemas operacionais** (Microsoft, Apple, Google, Mozilla, etc.);
- A CA deve estar em conformidade com os requisitos do **CA/Browser Forum** (Baseline Requirements e Guidelines para emissão de certificados SSL/TLS).

2. Tipo e Escopo (Wildcard)

- O certificado deve ser do tipo Wildcard, cobrindo o domínio principal e todos os seus subdomínios de primeiro nível;
- Exemplo: *.exemplo.com (cobre www.exemplo.com, api.exemplo.com, mail.exemplo.com, etc.);
- Não cobre subníveis adicionais (ex.: *.sub.exemplo.com --> não incluso).

3. Validação de Organização (OV)

- A emissão deve ser baseada em **validação de organização**, incluindo:
 - Verificação da existência legal da empresa/entidade solicitante;
 - Confirmação de endereço físico ou registros oficiais;
 - Validação de que a entidade tem direito sobre o domínio solicitado;
 - Inclusão do **nome da organização** como **Subject** do certificado.

4. Características Técnicas

- Certificado no padrão X.509 v3;
- Criptografia assimétrica com chave privada com tamanho mínimo de 2048 bits RSA ou curva elíptica ECC P-256/P-384, conforme boas práticas de segurança atuais;
- Algoritmos de assinatura: SHA-256 (ou superior);
- Suporte a protocolos de segurança TLS 1.2 e 1.3;
- Deve ser entregue em formatos compatíveis com servidores web/aplicações (ex.: .crt, .pem, .pfx).

5. Compatibilidade e Reconhecimento

- O certificado deve ser reconhecido nativamente por todos os principais navegadores **web, sistemas operacionais, dispositivos móveis e servidores**, sem necessidade de instalação manual de raiz.

6. Validade

- O certificado deve possuir validade de **1 (um) ano**, em conformidade com as regras internacionais vigentes (CA/B Forum, a partir de setembro/2020).

7. Suporte a Revogação e Transparência

- Deve permitir validação via **CRL (Certificate Revocation List)** e **OCSP (Online Certificate Status Protocol)**;
- O certificado deve ser publicado em **CT Logs (Certificate Transparency)**, conforme exigência de navegadores modernos.

1.2. Requisitos de Capacitação (art. 3º, II c/c art. 4º, IV)

Não há necessidade, visto que o TRE-MA já utiliza a solução.

1.3. Requisitos Legais

A contratação deverá observar as seguintes leis e normas:

- [Resolução CNJ 370/2021](#), que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- [Resolução CNJ 396/2021](#), que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- [Resolução TSE 23.644/2021](#), que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- [Resolução TRE-MA 9.846/2021](#), que dispõe sobre o Plano Estratégico para o sexênio 2021-2026;
- [Plano Diretor de Tecnologia da Informação e Comunicação](#) (2021-2026);
- [Plano Anual de Contratações de Soluções da STIC 2025](#);
- [Portaria CNJ Nº 162/2021](#), que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;
- [Lei nº 13.709/2018](#), Lei Geral de Proteção de Dados Pessoais – LGPD, quanto à segurança, guarda e tratamento de dados pessoais no ciclo de backup e restauração;
- [Lei Nº 14.133/2021](#), Lei de Licitações e Contratos Administrativos;
- [Resolução CNJ nº 468/2022](#), que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação.
- Todas normas regulatórias do ICP-BRASIL.

1.4. Modalidade e tipo de licitação

Com a implantação do Processo Judicial Eletrônico na Justiça Eleitoral (PJe) permitiu o uso racional e inteligente da tecnologia em favor de uma Justiça Eleitoral mais célere, acessível, econômica, eficiente e sintonizada com a preservação ambiental.

Portanto, é imprescindível o uso de certificação digital para uso do PJe, SERASA-JUD, SIAFI e RENAJUD por parte dos usuários (magistrado e servidores) para a sua plena operação, bem como os documentos gerados por estes, tenham a sua autenticidade comprovada. Essa comprovação é garantida mediante certificados digitais pessoais do tipo A3. Esses certificados precisam ser gerados e armazenados em nuvem para atender às normas da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Assim, torna-se imperiosa a existência de serviço de emissão de certificados digitais para magistrados e para servidores a fim de garantir a manutenção dos certificados ativos, bem como mitigar o risco, na situação de perda, roubo, dano, uso incorreto (esquecimento de senha, etc.) ou expiração da validade do certificado digital o usuário fique impossibilitado de utilizar os sistemas e processos que apoiam as atividades finais e administrativos deste Tribunal.

Considerando que o método aplicado para esta contratação será o da demanda por escopo, onde o TREMA, na função de CONTRATANTE, define em contrato as atividades a serem executadas, os resultados esperados, os padrões de qualidade exigidos e os procedimentos de execução em conformidade com os adotados pela organização, cabendo à pretendente CONTRATADA estipular o custo.

Considerando que o Sistema de Registro de Preços é um aliado dos princípios da eficiência e da economicidade, por ser um procedimento que resulta em vantagens à Administração, como a desburocratização das aquisições, redução do volume de estoque, redução da quantidade de licitações, propicia e facilita um maior número de ofertantes, inclusive a participação das pequenas e médias empresas, enxuga os gastos do erário.

A presente contratação não se pode determinar com precisão a demanda futura em virtude da imprevisibilidade gerada por fato

superveniente como posse de servidores e magistrados, perda, roubo dos certificados já emitidos.

Desta forma, pode-se concluir que a melhor opção é “**Pregão Eletrônico**” do tipo “**Menor Preço**” através do **Sistema de Registro de Preço**.

1.5. Requisitos Temporais

- O Contrato terá vigência de 36 (trinta) meses conforme art. 107 da Lei nº 14.133/2021, onde ele deve vigorar pelo período suficiente para entrega, instalação e o fim da validade do certificado digital; que no caso do certificado tipo A3 é de três anos.

- Da disponibilização do certificado digital:

O prazo para a emissão e disponibilização do certificado digital será de até 10 (dez) dias úteis, contados a partir do primeiro dia útil após a solicitação enviada pelo Gestor do Contrato.

1.6. Requisitos de sustentabilidade

- A contratada deverá utilizar exclusivamente processos digitais e eletrônicos para a emissão, validação e renovação e suporte dos certificados;
- Todos os documentos, termos, manuais, dentre outros devem ser fornecidos ao TRE/MA em formato eletrônico;
- Serão contratadas, preferencialmente, empresas que adotem práticas de eficiência energética em sua operação e infraestrutura de Tecnologia da Informação (TI) - a comprovação de eficiência energética poderá ser realizada por meio de certificações formais, laudos, relatórios de PUE ou contratos de fornecimento de energia renovável;

1.7. Requisitos de capacidade técnica e qualificação econômico-financeira

1.7.1. Documento que ateste que a licitante é autorizada a emitir certificados digitais e é credenciada perante o Instituto Nacional de Tecnologia da Informação (ITI) ou Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.7.1.1. Será vedada a habilitação de empresas em fase de credenciamento.

1.7.1.2. São consideradas como pertencentes ao mesmo grupo empresarial da proponente empresas por ela controladas ou empresas controladoras da proponente, ou empresas que tenham, no mínimo, uma mesma pessoa física ou jurídica que seja sócio da empresa emitente do atestado e da proponente.

1.7.2. Atestado(s) de capacidade técnica, emitido por pessoa jurídica de direito Público ou Privado ou regularmente emitido pelo conselho profissional competente quando for o caso, em nome da Contratada, em papel timbrado devidamente assinado e com identificação do emitente. O(s) Atestado(s) deverá(ão):

- Comprovando que a Licitante executou ou está executando, serviço de emissão de certificados digitais para, no mínimo, 60 certificados em território Brasileiro;
- Será permitido o somatório de atestado;

1.7.3. Para fins da comprovação de que trata o subitem anterior, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

- Amplo conhecimento no desenvolvimento do tema em que será prestado o serviço;
- Comprovar a experiência mínima de 3 (três) anos na prestação dos serviços pertinentes, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de serem ininterruptos;
- Conter o nome, o endereço, o telefone dos atestadores, ou qualquer outra forma de que a Administração possa valer-se para manter contato com os declarantes;
- Se emitido(s) por pessoa jurídica de direito público deverá(ão) ser assinado(s) pelo responsável do setor competente do Órgão, devidamente identificado (nome, cargo, CPF ou matrícula);
- Ser emitido por empresa que não integre o mesmo grupo empresarial da empresa proponente;
- Serão consideradas como pertencentes ao mesmo grupo empresarial, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio, proprietário ou titular da empresa emitente e da empresa proponente;
- Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante;
- Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do interessado.

1.7.4. Documento que ateste a aptidão econômica-financeira do licitante:

1.7.5. Certidão negativa de falência, expedida pelo cartório distribuidor da sede da Contratada.

1.7.6. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede da Contratada, caso se trate de pessoa física, desde que admitida a sua participação na licitação ou de sociedade simples.

1.7.7. Balanço patrimonial e demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios, que comprovem a boa situação financeira

2. ESTIMATIVA DAS QUANTIDADES - Justificativa de Dimensionamento da Demanda de Certificados Digitais (2026-2028)

O planejamento da presente contratação visa suprir a demanda de certificados digitais (**e-CNPJ** - Tipo A1, **e-CPF** - Tipo A3 e **SSL/TLS Wildcard OV**) para os próximos **três anos (2026 a 2028)**. A análise de expiração e a necessidade de novos certificados sustentam o quantitativo solicitado:

1. Certificados Tipo A3 (e-CPF)

A maior demanda concentra-se nos certificados Tipo A3 (e-CPF). O Tribunal possui atualmente **71** certificados A3 disponíveis.

- **Expiração Programada:** Estão previstas as expirações de **43** certificados A3 em **2026** e de **35** certificados A3 em **2027**.
- **Demanda Nova:** É estimada a necessidade de emissão de **40** novos certificados A3 por ano, totalizando **120** ao longo de três anos.
- **Total Requerido:** O quantitativo de **120 certificados Tipo A3** é necessário para o triênio, garantindo a substituição dos certificados que expiram e a disponibilidade para novos usuários/demandas.

2. Certificados Tipo A1 (e-CNPJ) e Wildcard (SSL/TLS)

A contratação é planejada para garantir a certificação do Tribunal por um período de três anos.

- **Expiração Programada:** Em cada um dos anos (**2026** e **2027**), irá expirar **um** certificado Tipo A1 (**e-CNPJ**) e **um** certificado Tipo Wildcard.
- **Total Requerido:** A demanda total é de **4** certificados Tipo A1 e **4** certificados Tipo Wildcard, visando a cobertura completa do triênio.

3. PREVISÃO DA CONTRATAÇÃO

Esta contratação está prevista no Plano de Contratações da Secretaria de Tecnologia de Informação do TRE-MA/2025, correspondendo ao item 66 do referido plano, localizado no sítio: <https://www.tre-ma.jus.br/institucional/governanca-gestao/governanca-de-tecnologia-da-informacao/planejamento-tatico-operacional/arquivos/plano-anual-de-contratacoes-de-tic-2025-2a-revisao>.

4. AVALIAÇÃO DE SOLUÇÕES

Solução 1 - Contratar o serviço de emissão de certificados por empresa especializada.

Vantagens:

- Atende a demanda por certificados digitais sem a necessidade de dispêndio em recursos de infraestrutura tecnológica, gestão e operacionalização do processo de certificação digital.
- Controle do processo de certificação digital das autoridades certificadoras garantem que os certificados digitais adquiridos estejam em conformidade com os padrões de mercado, com a legislação e normas vigentes, sobretudo as normas que regem a utilização dos sistemas informatizados utilizados na Justiça Eleitoral.
- Manutenção da viabilidade de fornecimento, sob demanda, durante a vigência do contrato.

Desvantagens:

- O processo de validação e emissão dos certificados digitais é realizado por um preposto da contratada, fora do ambiente físico do Tribunal, além de ser bastante burocrático, em razão da validação presencial.
- Custo indireto ao erário, relativo às despesas de deslocamento e devido à indisponibilidade do servidor ou magistrado para outras atividades.

Solução 2 - Criação de Autoridade Certificadora da Justiça Eleitoral do MA vinculada à ICP-Brasil

Vantagens:

- Supre satisfatoriamente a demanda por certificados digitais.
- Rigoroso controle do processo de certificação digital, garantindo que os certificados digitais emitidos estejam em conformidade com os padrões de mercado, com a legislação e normas vigentes, sobretudo as normas que regem a utilização dos sistemas informatizados utilizados na Justiça Eleitoral e externos a ela.

Desvantagens:

- Alto custo de implantação;
- Alto custo de manutenção anual da infraestrutura física, tecnológica e de pessoal.

- Requer planejamento, com tempo de implantação estimado entre 1 a 2 anos, e investimento por longo prazo;
- Requer atualização tecnológica periódica a cada 05 anos aproximadamente;
- Indispensável manter toda a infraestrutura necessária pelo período de validade de seus certificados, que no caso das de AC de 1ª nível vinculadas à ICP-Brasil é de 13 (treze) anos ou, ao menos, pelo período de validade dos certificados que tenham sido emitidos por esta AC, sob pena de sofrer as responsabilidades civis decorrentes.

● ESTIMATIVA DE CUSTO DA SOLUÇÃO

Foi realizada uma pesquisa de preços no mercado (internet) e banco de preços, doc. nº 2575184 para subsidiar a estimativa dos custos dos itens especificados no estudo.

Para estimar o custo total da contratação utilizando como parâmetro a mediana do referido documento e a estimativa de demanda (item 2), temos a tabela abaixo com os valores:

Produto/Especificação	Quantidade	Valor Unitário	Valor de Referência
Serviço de validação e emissão de Certificado Tipo A1 (e-CNPJ)	4	R\$ 230,00	R\$ 920,00
Serviço de validação e emissão de Certificado Tipo A3 (e-CPF) em Nuvem	120	R\$ 130,00	R\$ 15.600,00
Serviço de validação e emissão Certificado SSL/TLS Wildcard OV (Organizational Validation)	4	R\$ 1.502,95	R\$ 6.011,80
VALOR TOTAL			R\$ 22.531,80

Portanto, temos um custo estimado total de **R\$ 22.531,80 (vinte e dois mil, quinhentos e trinta e um reais e oitenta centavos)**.

5. ESCOLHA DA SOLUÇÃO

A Solução 1 apresenta menor custo e é a solução já reconhecida no mercado, amplamente aceita e com segurança e credibilidade garantida pelo rigoroso processo de credenciamento e auditoria das ACs por parte da ICP-Brasil. A outra solução avaliada, além de maior custo, demandaria bastante tempo entre o planejamento e a implantação.

Dessa forma, optou-se pela adoção imediata da Solução 1 – Contratação de serviço de emissão de Certificados Digitais.

6. NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE

- 6.1. Quanto a infraestrutura tecnológica
Não se aplica.
- 6.2. Quanto a infraestrutura elétrica
Não se aplica.
- 6.3. Quanto a logística de implantação
Não se aplica.
- 6.4. Quanto ao espaço físico
Não se aplica.
- 6.5. Quanto ao mobiliário
Não se aplica.
- 6.6. Quanto ao impacto ambiental

Observa-se que a prestação do serviço de emissão de certificados digitais produz impactos positivos ao meio ambiente ao promover a diminuição do uso de papel e o de tinta de impressão como principal suporte físico dos processos. O Certificado Digital se torna um relevante aliado na luta pela preservação do meio ambiente. O uso de documentos eletrônicos também contribui para reduzir o impacto ambiental das atividades econômicas eliminando a emissão de gases poluentes provenientes do transporte de documentos e reduzindo sensivelmente a necessidade de construção de grandes áreas de armazenamento de papel.

7. DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

- 7.1. TRE - Gestor do Contrato - Gestão do contrato, pagamento e qualidade dos serviços
7.2. TRE - Fiscal administrativo - Gestão orçamentária do contrato e gestão administrativa.
7.3. TRE - Fiscal técnico - Acompanhamento da execução dos serviços pela CONTRATADA, dar aceite aos serviços prestados.
7.4. CONTRATADA - Técnico especializado na emissão de certificado digital e recursos necessários para implementação da solução deverão ser fornecidos pela contratada.

8. DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DO CONTRATO

8.1. Quanto a entrega das versões finais dos produtos e da documentação alvos da contratação

Não se aplica.

8.2. Quanto a transferência final de conhecimentos sobre a execução e a manutenção da solução de TIC

Não se aplica.

8.3. Quanto a devolução de recursos materiais

Não há previsão de necessidade de entrega de recursos materiais para a empresa fornecerá os serviços.

9. ELABORAÇÃO DA ESTRATÉGIA DE INDEPENDÊNCIA

9.1. Quanto a forma de transferência de conhecimento tecnológico (contratação de desenvolvimento de softwares sob encomenda no mercado de TIC)

Não há necessidade de previsão de transição contratual, uma vez que não há impacto relevante, pois há várias empresas no mercado que oferecem serviço de emissão de certificados digitais e sua falta não impedirá o funcionamento dos certificados já emitidos, restando prejudicada apenas a emissão de novos certificados até que outro contrato seja firmado.

9.2. Quanto aos direitos de propriedade intelectual e autorais da solução de TIC

Não se aplica.

9.3. Quanto à documentação e afins pertinentes à tecnologia de concepção, manutenção e atualização, bem como, quando cabível, do código fonte junto à Autoridade Brasileira que controla a propriedade intelectual de softwares, para garantia da continuidade dos serviços, em caso de rescisão contratual, descontinuidade do produto comercializado ou encerramento das atividades da contratada, quando da contratação de desenvolvimento de sistemas de informação considerados estratégicos.

Não se aplica.

10. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO

10.1. Para a contratação pretendida foram consideradas as características técnicas e peculiares de comercialização no mercado, avaliando-se o objeto em conformidade com o Princípio do Parcelamento, nos termos do Art. 40, §§ 2º e 3º da Lei Federal nº 14.133 de abril de 2021.

10.2. A presente contratação será realizada com a adjudicação do objeto em um único grupo.

10.3. A seguir são apresentadas evidências e informações que subsidiaram a decisão de agrupamento dos itens, nos termos do item 10.2:

10.3.1. Os itens foram agrupados em grupo único em razão de, além de possuírem mesma natureza, gerar economia processual e de escala, haja vista que o baixo valor individual poderia não atrair fornecedores, sendo o valor global uma motivação para o surgimento de interessados.

10.3.2. A contratação em um único procedimento também tem como objetivo atender ao princípio da economicidade, por promover o melhor resultado estratégico possível de uma determinada alocação de recurso financeiro, considerando que o procedimento único não inviabilizará a concorrência, pois existem diversos fornecedores que possuem condições de entregar os itens propostos.

10.3.3. A contratação será realizada por grupo único em razão da conexão e similaridade dos certificados digitais, o que favorece a obtenção da melhor proposta global e otimiza a gestão contratual. A simples discriminação em 03 (três) itens visa apenas à identificação precisa de cada tipo de certificado e o controle de seus quantitativos, não configurando parcelamento indevido nem frustrando a competitividade do certame.

10.3.4. Desta forma, evitando prejuízo ao conjunto do objeto a ser adquirido, esta licitação será realizada em grupo único.

11. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

11.1. Trata-se o objeto de produtos com características comuns e usuais encontrados no mercado de tecnologia da informação, cujos padrões de definição, desempenho e de qualidade podem ser

objetivamente definidos.

11.2. A presente contratação tem por objeto a contratação de serviço de validação e emissão de certificados digitais do tipo A3 Pessoa Física com armazenamento em nuvem - todos com validade

de 3 anos, certificados do tipo A1 e-CNPJ Pessoa Jurídica com validade de 1 ano e certificados do tipo SSL do tipo WILDCARD OV com validade de 1 ano.

11.3. A contratação de serviços de emissão de certificado digital em nuvem visa permitir o seu uso em múltiplos dispositivos, incluindo dispositivos móveis, e a sua recuperação em caso de perda de dispositivo.

11.4. Tecnicamente, busca-se com a contratação: permitir que os servidores do TRE-MA que necessitem assinar documentos digitalmente, o façam com a possibilidade de uso de seus dispositivos móveis tendo suas assinaturas digitais armazenadas em nuvem para que haja possibilidade de recuperação.

11.5. Com vistas a garantir a continuidade dos processos e trâmites que requerem assinatura digital de servidores, faz-se necessário a contratação do objeto deste estudo, levando em consideração os princípios norteadores da Administração Pública, tais como eficiência e economicidade.

11.6. Todos os elementos necessários à prestação do serviço estarão dispostos no Termo de Referência, entre eles as obrigações e responsabilidades da contratada e especificações técnicas do serviço.

11.7. A solução de ter prestação de suporte técnico remoto, via telefone, e-mail, chat e/ou website, por equipe de técnicos especializados, para esclarecimento de dúvidas técnicas e cadastrais.

12. CONCLUSÃO DOS ESTUDOS PRELIMINARES

Declaramos a viabilidade da contratação com base nas informações levantadas neste documento.



Documento assinado eletronicamente por **LOURENCIO MONTEIRO DE MELO, Analista Judiciário**, em 23/10/2025, às 15:17, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **MARIA TERESA DA COSTA PEDROSA, Analista Judiciário**, em 23/10/2025, às 15:32, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **EGÍDIO DE CARVALHO RIBEIRO JÚNIOR, Coordenador(a)**, em 23/10/2025, às 15:40, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **JOSÉ WAGNER SALES FERREIRA, Secretário(a)**, em 23/10/2025, às 17:47, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.tre-ma.jus.br/autenticar> informando o código verificador **2599815** e o código CRC **DFAB153A**.

0010154-06.2025.6.27.8000	2599815v3
---------------------------	-----------