Estudos Preliminares da STIC Nº 5/2023 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (art. 14)

Contratação do serviço continuado de emissão de CERTIFICADOS DIGITAIS para atender todas às necessidades do **Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça, Vice-Ccorregedoria Geral de Justiça e a Escola Judiciária – EJUD**

1. Requisitos da contratação

De início, resta necessário definir com base na necessidade do TJPI quais as principais características que a solução deve atender. Nesse sentido e em atenção à Resolução CNJ nº 182/2013, procede-se à definição das necessidades mínimas que se espera atender com a aquisição da solução de TIC objeto deste Estudo.

1.1 Necessidades do negócio

Com vias a melhor instruir o processo em epígrafe, bem como subsidiar a confecção do Termo de Referência, procede-se à listagem das principais necessidades com suas respectivas funcionalidades a serem atendidas com a contratação pretendida.

1.1.1. Necessidade 1: garantir a validade jurídica, autenticidade, integridade e não repúdio dos documentos expedidos pelo TJPI.

1.1.1.1. Funcionalidade 1: Resguardar a autoria e a legitimidade de documentos eletrônicos.

1.1.1.2. Funcionalidade 2: Promover proteção contra alterações não autorizadas em documentos eletrônicos.

1.1.1.3. Funcionalidade 3: Impedir que o autor de documentos digitalmente assinados recuse ou conteste sua autoria.

1.1.1.4. Funcionalidade 4: Identificar com segurança os sistemas hospedados pelo TJPI através de protocolo de comunicação seguro (HTTPS).

1.1.2. Necessidade 2: Adicionar segurança SSL ao domínio e subdomínios do TJPI.

1.1.2.1. Funcionalidade 1: Implementar segurança SSL nos sites que fazem parte do subdomínio "TJPI.JUS.BR"

1.1.3. Necessidade 3: manter a disponibilidade dos certificados digitais utilizados para assinatura de documentos.

1.1.3.1. Funcionalidade 1: Renovar os certificados de assinatura conforme estes forem alcançando seu prazo de validade.

1.1.4.2. Funcionalidade 2: Prover certificados digitais para eventuais novos magistrados ou servidores.

1.1.3. Necessidade 3: Compatibilidade com as mídias criptográficas em estoque no TJPI. .

1.1.3.1. Funcionalidade 1: Os novos certificados digitais dever ser compatíveis com as mídias criptográficas que o TJPI adquiriu em contratos anteriores.

1.1.4. Atores envolvidos: para o projeto em epígrafe ficam destinadas as seguintes partes fundamentais:

1.1.4.1. Gerente de projetos da CONTRATANTE: servidor indicado pela autoridade competente do TJPI para liderar o projeto de contratação da solução bem como atestar a regularidade das fases pertinentes e manter contato direto com o preposto da CONTRATADA.

1.1.4.2. Gerente de projetos da CONTRATADA: preposto indicado pela empresa fornecedora da solução com funções de gerência e/ou liderança que deverá manter contato direto com o gerente de projetos da CONTRATADA em todas as fases do projeto com o fito de garantir a regularidade da aquisição.

1.1.4.3. Analistas de TIC do setor de Infraestrutura e Segurança da Informação da STIC com a função de descrever os requisitos técnicos bem como testar e homologar a conformidade do fornecimento da solução em aderência aos padrões descritos.

1.2. Requisitos não funcionais/tecnológicos

1.2.1. Requisitos de capacitação:

Como se trata de solução de certificação digital, não há necessidade de treinamento/capacitação para a contratação em epígrafe.

1.2.2. Requisitos legais:

Esta contratação busca atender as necessidades do PJPI, obedecendo rigorosamente às legislações federal e estadual pertinentes, às Resoluções do CNJ, bem como aos instrumentos legais emitidos pelos órgãos avaliadores de conformidade como a Associação Brasileira de Normas Técnicas – ABNT, o Instituto Nacional de Metrologia, Qualidade e Tecnologia – INMETRO, Instituto Brasileiro de Meio Ambiente – IBAMA, dentre outros.

No que tange à legislação específica, não fora encontrada nenhuma observância obrigatória para o projeto em epígrafe.

1.2.3. Requisitos de manutenção:

1.2.3.1. Requisito 2: Níveis de serviços exigidos (NSE) para certificados digitais:

a) Os Níveis de Serviços Exigidos (NSE) serão classificados conforme os níveis de criticidade a seguir:

Prazo de resposta	
Criticidade ALTA	24 (vinte e quatro) horas
Criticidade MÉDIA	48 (quarenta e oito) horas
Criticidade BAIXA	72 (setenta e duas) horas

i. Criticidade ALTA: Esse nível de criticidade é aplicado quando o certificado SSL for considerado inseguro e/ou recusado pela Infraestrutura de Chaves Públicas da hierarquia a qual pertence ou quando não for possível realizar assinatura de documentos com os certificados do tipo A;

ii. Criticidade MÉDIA: Esse nível de criticidade é aplicado quando há recusa de autenticação do certificado por alguma outra infraestrutura de chaves públicas que não seja a da hierarquia a qual pertence o certificado;

iii. Criticidade BAIXA: Esse nível de criticidade é aplicado para a instalação, configuração, manutenção, esclarecimentos técnicos relativos ao uso e documentação do certificado, bem como chamados técnicos que não requeiram imediatos atendimentos.

b) Os Níveis de Serviços Exigidos (NSE) serão tratados da seguinte forma:

i. Prazo de Solução Definitiva: Tempo decorrido entre o envio da mensagem de chamado técnico efetuado pelo Fiscal Técnico ou Gestor do Contrato, e a efetiva recolocação da solução em seu pleno estado de funcionamento. Poderá ser de, no máximo, cinco vezes o tempo do prazo de resposta a depender da criticidade exposta no item anterior;

ii. Caso seja verificado que a solução apresentada pela empresa não resolveu o problema definitivamente, o chamado será reaberto pelo Fiscal Técnico ou Gestor do Contrato e o prazo continuará a ser contado a partir do momento de sua interrupção.

1.2.4. Requisitos temporais

1.2.4.1. Planejamento do processo de aquisição por parte da equipe de planejamento da contratação: para garantir eficiência no processo de contratação, ficam definidos um prazo máximo de 15 (quinze) dias úteis para cada uma das seguintes fases:

i. Planejamento interno da contratação a ser realizado pela equipe de contratação;

ii. Tramitação processual, incluindo aprovação da demanda por parte da autoridade competente;

iii. Aprovação da aquisição por parte da autoridade máxima do TJPI;

iv. Contratação do fornecedor.

1.2.4.2. Prazo de fornecimento dos certificados A1 Cert-JUS e wildcard SSL: a CONTRATADA deverá emitir os certificados em, no máximo, 01 (um) dia útil após a realização da visita presencial (ou por videoconferência) ou agendamento para coleta de assinaturas e validação de documentos. O certificado deverá ser emitido pela internet, por meio de link para download.

1.2.4.3. Prazo de fornecimento dos certificados A3 Cert-JUS: o certificado deverá ser emitido durante a visita presencial (ou por videoconferência). O certificado deverá ser gravado na mídia criptográfica do magistrado/servidor (caso este já tenha uma) ou em um novo token USB (caso o magistrado/servidor não possua a mídia).

1.2.4.4. Prazo de verificação de compatibilidade com as mídias criptográficas: a CONTRATADA deverá realizar os testes de compatibilidade no prazo máximo de 05 (cinco) dias úteis.

1.2.4.5. Prazo para realização de visita técnica: deverá ser de até 05 (cinco) dias úteis contados a partir do recebimento do pedido de visita por parte do TJPI.

1.2.4.5. Prazo para emissão do termo de recebimento definitivo ou documento equivalente: em até 15 (quinze) dias úteis do recebimento do pedido de pagamento e notas fiscais a equipe de planejamento da contratação fornecerá o termo de recebimento definitivo atestando a regularidade do fornecimento.

1.2.5. Requisitos de segurança

A solução deve estar em conformidade com as políticas de Segurança da Informação do Tribunal de Justiça do Piauí, bem como com os procedimentos e documentações exigidas.

Todas as informações consideradas sensíveis pelo TJPI deverão ser resguardadas por parte da CONTRATANTE não sendo permitido, em hipótese alguma, o compartilhamento, cópia, retirada, reprodução, carga, levantamento, entre outros, de informações oriundas dos sistemas informatizados e/ou bancos de dados institucionais sem a devida autorização prévia e expressa por parte da autoridade competente do TJPI.

São consideradas sensíveis, para fins de aplicação do item anterior, aquelas informações que por sua natureza são consideradas de interesse confidencial, restrita ou sigilosa como, por exemplo:

- Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto ser divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo TJPI a tais documentos.
- Resultados, parciais ou totais, sobre produtos gerados.
- Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações.
- Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do TJPI e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de dados, versões “beta” de quaisquer programas, dentre outros.
- Documentos relativos à lista de usuários do TJPI e seus respectivos dados, armazenados sob qualquer forma.

- Metodologias e ferramentas de serviços, desenvolvidas pelo TJPI.
- Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do TJPI, sejam eles executados interna ou externamente.
- Parte ou totalidade dos dados ou informações armazenados nas bases de dados que subsidiam os sistemas de informações do TJPI, sejam elas residentes interna ou externamente.
- Circulares e comunicações internas do TJPI.
- Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo TJPI.

1.2.6. Requisitos sociais, ambientais e culturais

O fabricante da solução deverá atender aos critérios de sustentabilidade ambiental de que trata a Instrução Normativa SLTI/MPOG nº 01/2010, no que couber, quanto ao uso de materiais, observando que esses sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme Normas ABNT NBR – 15448-1 e 15448-2.

Deverão ser observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

1.2.7. Requisitos de compatibilidade técnica

Os Certificados digitais da cadeia AC-JUS A3 para pessoa física (Cert-JUS) devem ser compatíveis com os seguintes modelos de mídias criptográficas:

- **SafeNet 5100**
- **ePass2003**

1.3. Levantamento das alternativas disponíveis no mercado de TIC

De início, faz-se necessário tecer comentários acerca do que se pretende contratar. O Certificado digital funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

Como benefícios da utilização do certificado digital, pode-se listar:

- Assinatura de documentos e contratos digitais: os documentos assinados digitalmente com certificado digital ICP-Brasil têm a mesma validade que os documentos assinados em papel. Além de proporcionar economia de insumos, já que não há necessidade de realizar impressões, os documentos assinados digitalmente agilizam processos, pois podem ser enviados por e-mail e assinados de qualquer lugar facilmente;
- Categorias profissionais: diversas categorias profissionais (médicos, advogados, contadores, militares, entre outros) já utilizam o certificado digital em suas rotinas. Com o certificado, as classes profissionais têm a possibilidade de trabalhar com sistemas virtuais unificados e seguros, proporcionando integração e desburocratização de processos relativos ao setor;
- Autenticação em sistemas: existem vários sistemas com informações confidenciais, especialmente de governo, que só podem ser acessados presencialmente, através da confirmação de identidade. Como o certificado digital garante autenticidade, ele proporciona o acesso à esses sistemas e informações através da internet, não havendo necessidade de comparecimento presencial;
- Atualização de informações em sistemas: Além de garantir acesso seguro à sistemas, o certificado também permite a alteração rápida de informações, evitando longos processos burocráticos.

1.3.1. Soluções:

Com base nas informações já explicitadas, foram localizados no mercado de TIC os seguintes tipos de certificados digitais:

1. Tipo A (A1, A3, A4): certificado de assinatura digital. É o tipo mais utilizado de certificado digital e pode ser aplicado para conferir autenticidade a qualquer tipo de documento e arquivo virtual. Seu principal objetivo é identificar o assinante, confirmar a integridade do documento e atestar a autenticidade da operação realizada. Esse modelo de certificado é indicado para profissionais liberais, independentemente da área de atuação, que precisam realizar o envio de documentos digitais assinados. Organizações que têm um grande volume de validação de documentos também podem otimizar o trabalho utilizando-se desse certificado.
2. Tipo S (S1, S3, S4): certificado de sigilo/confidencialidade. É um modelo que busca trazer sigilo para uma determinada transação, já que, por meio de sua utilização, é possível criptografar os dados de um documento, que, a partir desse momento, só poderá ser acessado por meio de um certificado autorizado, evitando, assim, o vazamento de informações. Ou seja, ao utilizar o tipo S, o conteúdo do documento assinado se torna inacessível para pessoas que não tenham autorização e, com isso, é muito mais seguro transmitir informações sigilosas pela rede. Empresas que precisam trocar informações de cunho sigiloso constantemente podem se valer dessa proteção.
3. Tipo T (T3): certificado de tempo. É mais conhecido como carimbo de tempo, uma vez que seu objetivo é atestar quando um documento digital foi emitido, tornando evidente a data e a hora que determinada informação digital passou a existir. Como esses dados poderiam ser facilmente adulterados para beneficiar uma das partes, em uma ação judicial, por exemplo, o tipo T utiliza uma terceira parte certificadora para atestar o exato instante em que o documento foi emitido, evitando fraudes. Pode ser utilizado em conjunto com os demais certificados para garantir ainda mais segurança às transações.
4. e-CPF: principal documento de identificação de pessoa física, também tem uma versão digital para garantir a autenticidade das transações eletrônicas realizadas por pessoas físicas. É possível realizar várias ações em formato digital, como assinar contratos, criar procurações online e ter acesso ao site da Receita Federal. O e-CPF funciona com criptografia de dados, oferecendo segurança, sigilo e integridade de dados. Utiliza-se da mesma tecnologia do certificado A, podendo ser emitido com o tipo A1 ou A3.
5. e-CNPJ: principal identificação de pessoa jurídica no Brasil, garante a autenticidade e a integridade de transações de empresas no meio eletrônico. As organizações que têm um e-CNPJ podem fazer procurações, fechar contratos, entre outras ações que poderiam ser realizadas fora do ambiente virtual. Por exigência da Receita Federal, apenas o responsável direto pelo CNPJ da empresa poderá responder pelo e-CNPJ. Assim como o e-CPF, ele é emitido e armazenado utilizando os modelos A1 e A3.
6. NF-e: arquivo que garante a autoria e a validade jurídica das emissões de notas fiscais pela empresa aos órgãos responsáveis. O certificado digital NF-e pode ser atribuído diretamente a um funcionário, sem a necessidade de compartilhar o e-CNPJ da empresa, trazendo mais segurança para a operação. Assim como o e-CPF e e-CNPJ, ele é emitido e armazenado utilizando os modelos A1 e A3.
7. Certificado SSL: é um certificado digital que garante a autenticidade de web sites, além de possibilitar a privacidade e integridade na transmissão dos dados entre o cliente e o seu site, minimizando o risco de fraudes. Pela importância desta segurança, a maioria dos navegadores está identificando como "Não-Seguro" os sites que estão sem o SSL ou com SSL configurado de forma incorreta. Divide-se em certificados para um único domínio ou para mais de um domínio/subdomínio.

Ainda, no caso específico do Poder Judiciário, existe uma cadeia denominada AC-JUS que emite certificados para pessoas físicas e as identificam como agentes públicos de determinado órgão do Poder Judiciário, e contém as informações de cargo, lotação e matrícula no órgão que representam. São, na prática, carteiras de identidade funcionais digitais dos servidores e magistrados. Assim, uma assinatura digital produzida com o uso de um certificado Cert-JUS equivale à assinatura manuscrita do agente

público, acompanhada de seu carimbo institucional. No Brasil, os certificados do tipo Cert-JUS podem ser expedidos somente por Autoridades de Registro - AR autorizadas pela Autoridade Certificadora da Justiça - AC-JUS, conforme consta no seu site institucional (https://acjus.jus.br/). A AC-JUS é uma entidade instituída pela Resolução Conjunta nº 001, do Superior Tribunal de Justiça e Conselho da Justiça Federal em 20 de Dezembro de 2004 e que funciona como Autoridade Certificadora de primeiro nível vinculada à Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (AC Raiz).

Conforme assentado nas necessidades descritas no item 1 deste documento, a demanda em tela visa garantir a validade jurídica, autenticidade, integridade e não repúdio dos documentos expedidos pelo TJPI bem como adicionar segurança SSL ao domínio e subdomínios do TJPI. Nessa toada, os certificados do tipo A (certificado de assinatura) e SSL wildcard (curinga) são os indicados para atendimento da demanda em epígrafe.

Em tempo, ressalta-se que a realização de visita técnica bem como os testes de compatibilidade são acessórios esperados e necessários no fornecimento do objeto principal, qual seja: aquisição de certificados digitais. Assim, devem figurar no processo em epígrafe.

1.3.2. Análise dos custos totais das soluções de TIC identificadas (art. 14, III)

A tabela abaixo resume os valores unitários e médio apurados em pesquisa no sítio https://www.comprasgovernamentais.gov.br/ e no Sistema Banco de Preços dos items identificados anteriormente:

Apresenta-se, abaixo, tabela consolidando todos os custos totais apurados e suas respectivas médias e valor total estimado da contratação:

ITEM	ESPECIFICAÇÃO DO OBJETO	QUANTIDADE	VALOR UNITÁRIO	TOTAL
01	Emissão de Certificado Digital A3, sem Token Pessoa Física	3000	R$ 24,900	R$ 74.700,00
02	Mídia Criptográfica para Certificado Digital	3000	R$ 53,30	R$ 159.900,00
03	Emissão de Certificado Digital A1 para Pessoa Jurídica	16	R$ 55,997	R$ 895,95
04	Emissão de Certificado Digital A3 pessoa júridica	5	R$ 45,000	R$ 225,00
05	Emissão de Certificado Digital A1 para Equipamento Servidor	3	R$ 1.047,997	R$ 3.143,99
06	Serviço de Vistoria / Validação / Certificação	60	R$ 28,800	R$ 1.728,00
TOTAL				R$ 240.592,94

2. Detalhamento das alternativas existentes

DETALHAMENTO DAS ALTERNATIVAS EXISTENTES				
Requisito	**Nome da Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública (art. 14, II, a)?	Certificado digital tipo A	x		
	Certificado wildcard SSL	x		
	Mídia Criptográfica para Certificado Digital	x		

A Solução encontra-se implantada em outro órgão ou entidade do Judiciário?	Certificado digital tipo A	x		
	Certificado wildcard SSL	x		
	Mídia Criptográfica para Certificado Digital	X		
A Solução existe no Portal de Software Público Brasileiro (art. 14, II, b)?	Certificado digital tipo A			x
	Certificado wildcard SSL			x
	Mídia Criptográfica para Certificado Digital			X
A Solução é um software livre ou software público (art. 14, II, c)?	Certificado digital tipo A			x
	Certificado wildcard SSL			x
	Mídia Criptográfica para Certificado Digital			X
A Solução observa as políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário (art. 14, II, d)?	Certificado digital tipo A			x
	Certificado wildcard SSL			x
	Mídia Criptográfica para Certificado Digital			X
Caso haja necessidade de certificação digital, a Solução é aderente às regulamentações da ICP-Brasil (art. 14, II, e)?	Certificado digital tipo A	x		
	Certificado wildcard SSL		x	
	Mídia Criptográfica para Certificado Digital			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus (art. 14, II, f)?	Certificado digital tipo A			x
	Certificado wildcard SSL			x
	Mídia Criptográfica para Certificado Digital			X

3. Justificativa da solução escolhida (art. 14, IV)

3.1. Solução escolhida: Certificados digitais Tipo A, SSL wildcard e Mídia Criptográficas para Certificado Digital

3.2. Descrição (art. 14, IV, a):

O certificado digital SSL, via de regra, é emitido para um único endereço (exemplo: www.tjpi.jus.br). Ao utilizar o certificado SSL wildcard é possível adicionar segurança SSL em ilimitados sites e servidores, desde que estes pertençam ao subdomínio do mesmo domínio. Utilizando apenas um certificado digital SSL wildcard garante-se a proteção ao site principal (exemplo: www.tjpi.jus.br) e todos os seus subdomínios (exemplo: http://sei.tjpi.jus.br/, http://licitacoes.tjpi.jus.br/, http://transparencia.tjpi.jus.br/).

O certificado SSL wildcard é emitido para *.tjpi.jus.br, ou seja, é possível trocar o * por qualquer nome e utilizar segurança SSL em todos os subdomínios do TJPI. Com o certificado SSL wildcard é possível atingir elevado nível de eficiência ao adquirir apenas um certificado digital para qualquer subdomínio atual ou futuro do TJPI além de obter maior flexibilidade na configuração e gerenciamento dos sites e servidores.

Já os certificados digitais A é utilizado para realizar assinaturas digitais, identificando o titular, atestando a autenticidade da operação e confirmando a integridade do documento assinado. Ou seja, tudo o que for feito por meio do Certificado tem validade jurídica. A diferença do A1 para o A3 reside no fato que o A1 é instalado em um computador local, podendo ser realizadas cópias de segurança deste. Quanto ao A3, este é armazenado em um dispositivo criptográfico, que pode ser um token ou cartão inteligente.

E as Mídia Criptográfica para Certificado Digital são os equipamentos onde os certificados do tipo A são gravados para utilização por parte dos usuários.

3.3. Composição da solução (art. 14, IV, a):

Para a solução em apreço, sugere-se a seguinte composição com o respectivo GRUPO E ITENS:

GRUPO	ITEM	ESPECIFICAÇÃO DO OBJETO	QUANTIDADE	Validade	CATSER
GRUPO 01	01	Emissão de Certificado Digital A3, sem Token Pessoa Física	3000	03 (três) anos	27219
	02	Mídia Criptográfica para Certificado Digital	3000	GARANTIA 12 MESES	600120 (catmat)
	03	Emissão de Certificado Digital A1 para Pessoa Jurídica	16	01 (um) ano	27162
	04	Emissão de Certificado Digital A3 pessoa júridica	5	03 (três) anos	27197
	05	Emissão de Certificado Digital A1 para Equipamento Servidor	3	01 (um) ano	27170
	06	Serviço de Vistoria / Validação / Certificação	60	-----	25470

3.4. Alinhamento em relação às necessidades (art. 14, IV, b):

3.4.1. Certificados digitais do tipo A: garante a validade jurídica, autenticidade, integridade e não repúdio dos documentos expedidos pelo TJPI.

3.4.2. Certificado digital SSL wildcard: adiciona segurança SSL aos subdomínios do *.tjpi.jus.br.

3.4.3. Mídia Criptográficas: Garante a substituição das mídias que necessitam ser substituídas devido ao desgaste natural.

3.5. Benefícios esperados (art. 14, IV, c): Com a contratação dos certificados digitais em tela pretende-se alcançar os seguintes benefícios:

- Garantir a autenticidade, integridade e não repúdio na comunicação dos atos e transmissões de documentos eletrônicos;
- Permitir a implementação atual e futura de sistemas interoperáveis seguros;
- Atender as normas da ICP-Brasil que regulam o uso de certificados como mecanismo para implementação e incremento da segurança da informação;
- Garantir a autenticidade e confiabilidade das movimentações processuais dos Processos Eletrônicos;
- Assegurar o não repúdio de atos e movimentações executadas via processo eletrônico;
- Atender a demanda atual e dos próximos doze meses de certificados digitais do TJPI.

3.6. Relação entre a demanda prevista e a quantidade a ser contratada (art. 14, IV, d):

A quantidade a ser contratada está de acordo com os documentos (3312038, 3388432, 3882543) emitidos pelos diversos setores da stic e suas necessidades.

No tocante aos certificados digitais A1 e A3 para pessoa jurídica, o quantitativo levou em conta a existência de quatro pessoas jurídicas diferentes neste Tribunal, qual sejam: TJPI, a CGJ, a VICECGJ e a EJUD.

Em tempo, afirme-se que os quantitativos aqui propostos não serão necessariamente utilizados quando da finalização do certame licitatório. Outrossim, serão consumidos conforme a demanda do órgão.

4. Necessidades de adequação do ambiente do órgão (art. 14, V):

Tipo	**Necessidade**
Infraestrutura tecnológica (art. 14, V, a)	Não há.
Infraestrutura elétrica (art. 14, V, b)	Não há.
Logística de implantação (art. 14, V, c)	Após a assinatura do contrato será realizada uma reunião de alinhamento com a contratada para definição das etapas de implantação com os respectivos prazos para entrega e requisitos para aceite.
Espaço físico (art. 14, V, d)	Não há.
Mobiliário (art. 14, V, e)	Não há.
Impacto ambiental (art. 14, V, f)	Não há.
Outros (opcional):	Não há.

SUSTENTAÇÃO DO CONTRATO (art. 15)

5. Recursos necessários à continuidade do objeto contratado (art. 15, I)

5.1. Recursos materiais:

A contratação da solução em epígrafe não necessita de recursos materiais adicionais aos já existentes no parque tecnológico do TJPI.

5.2. Recursos humanos:

5.2.1. Recurso 1: Equipe de Infraestrutura-STIC do TJPI.

5.2.1.1. Função: Operar e manter a solução de TIC em aderência às regras da governança e da alta administração do TJPI.

5.2.1.2. Responsabilidades:

- Manter a solução de TIC em funcionamento e garantir a segurança dos dados trafegados no ambiente corporativo do TJPI;
- Garantir a autenticidade dos sistemas do TJPI e contribuir com a segurança da informação no TJPI;
- Manter contato direto com a CONTRATADA quando do aparecimento de incidentes e/ou problemas na solução.

5.2.2. Recurso 2: Preposto da CONTRATADA e/ou fabricante da solução.

5.2.2.1. Função: Manter a solução de TIC em perfeito funcionamento independentemente da atuação da Equipe de Infraestrutura-STIC do TJPI.

5.2.2.2. Responsabilidades:

- Atender todas as requisições do TJPI em tempo hábil e de acordo com os níveis de serviço (ANS) acordados;
- Atualizar, sempre que necessário, os softwares integrantes e/ou componentes da solução de TIC;
- Manter a confidencialidade dos dados que tiver acesso em decorrência do contrato a ser firmado.

6. Estratégia de continuidade em eventual interrupção contratual (art. 15. II)

6.1. Evento 1: Impossibilidade da contratada continuar fornecendo a certificação.

6.1.1. Ação de contingência: Contratar outra empresa que forneça suporte à solução adquirida.

6.1.2. Responsável: Equipe de contratação.

6.2. Evento 2: Rescisão contratual por parte da Administração ou da CONTRATADA.

6.2.1. Ação de contingência: Contratar outra empresa que forneça suporte à solução adquirida.

6.2.2. Responsável: Equipe de contratação.

7. Ações para transição e encerramento contratual (art. 15, III)

Ação	**Responsável**	**Data de Início**	**Data de Fim**
Entrega de versões finais dos produtos alvos da contratação <art. 15, inc. III, a>	Contratada	A partir da emissão do termo de recebimento provisório	Até a emissão do termo de recebimento definitivo ou documento semelhante
Transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação <art. 15, inc. III, b>	Não há necessidade de transferência de conhecimento.		
Devolução de recursos materiais <art. 15, inc. III, c>	Não há necessidade de devolução de qualquer dos materiais contratados.		
Revogação de perfis de acesso <art. 15, inc. III, d>	Não há necessidade de criação de perfis de acesso.		
Eliminação de caixas postais <art. 15, inc. III, e>	Não serão criadas caixas postais além das já existentes no TJPI		

8. Estratégia de independência (art. 15, IV)

Como o objeto deste Estudo não é o desenvolvimento de software sob encomenda no mercado de TIC conforme previsto no art. 15, inc. IV da Resolução nº 182/2013 do CNJ, e sim a contratação do certificados digitais; não se vislumbra necessidade de transferência de conhecimento na forma prevista na Resolução retro.

Quanto aos direitos de propriedade intelectual, estes permanecerão de posse da empresa fabricante do produto a ser adquirido, não havendo transferência de direitos de propriedade em face de contratação, salvo os direitos de uso da solução contratada.

ESTRATÉGIA PARA CONTRATAÇÃO (art. 16)

9. Natureza do objeto (art. 16, I)

O objeto a ser contratado enquadra-se na categoria de serviços comuns de que tratam a Lei nº 10.520/02 e os Decretos nº 3.555/00 e nº 5.450/05, por possuir padrões de desempenho e características gerais e específicas que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado.

10. Parcelamento do objeto (art. 16, II)

Os itens do grupo 01 (certificados digitais, mídias e visitas técnicas) não podem ser fornecidos por empresas diferentes devido ao fato dos serviços agrupados estarem intrinsecamente relacionados. Por praxe, o mercado atende a este tipo de demanda entregando os serviços como uma solução indissociável, de modo a ser fornecido por uma só empresa. Desta forma, assegura-se a eficiência no emprego dos recursos financeiros para a prestação do serviço pretendido. Assim, entende-se que os itens do grupo 01 deverão estar agrupados no mesmo lote e entregues a uma única empresa.

11. Adjudicação do objeto (art. 16, III)

Tratando-se de serviços comuns, a adjudicação será feita para o licitante que apresentar menor valor por lote.

11.1 Procedimentos e critérios de aceitação

Para aceitação da proposta é necessário o cumprimento o de 100% dos itens: "1.1.3. Necessidade 3" , "1.1.3.1. Funcionalidade 1" e "1.2.7. Requisitos de compatibilidade técnica", a serem mensurados durante o teste de conformidade.

12. Modalidade e tipo de licitação (art. 16, IV)

Considerando que os bens e serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a utilização do sistema de pregão do tipo “menor preço”, na sua modalidade eletrônica.

13. Classificação e indicação orçamentária (art. 16, V)

Para atendimento da demanda objeto do presente processo, sugere-se a seguinte classificação orçamentária:

- Unidade Orçamentária: 040105 - FERMOJUPI
- Fonte: 118 - Recursos de Fundos Especiais

- Natureza da Despesa: 339040 - Serviços de Tecnológia.

Ressalta-se, outrossim, que a posterior informação por parte da Secretaria de Orçamento e Finanças deste TJPI terá a função de detalhar as naturezas em obediência à legislação vigente.

14. Vigência da garantia e da prestação dos serviços (art. 16, VI)

Os certificados digitais do tipo A, Mídias e wildcard SSL deverão ter garantia de correção e atualização pelo período de validade individual de cada um, contados a partir da data de emissão destes. Nesse item está incluído a atualização dos softwares integrantes da solução bem como o suporte nos moldes deslindados no item 1.2.3 deste Estudo.

15. Equipe de apoio à contratação (art. 16, VII)

Integrante Requisitante	Eucassio Gonçalves Lima Júnior	**Matrícula**	**3365**
E-mail	eucassio.lima@tjpi.jus.br	**Telefone**	86 3230-7869
Integrante Requisitante Suplente	José Rozendo de Sousa Teixeira Neto	**Matrícula**	**3423**
E-mail	jose.rozendo@tjpi.jus.br	**Telefone**	86 3230-7869
Integrante Técnico	Cristiano Santiago Girão	**Matrícula**	**27566**
E-mail	girao@tjpi.jus.br	**Telefone**	86 3230-7869
Integrante Técnico	Frederico Costa Chaves	**Matrícula**	**3456**
E-mail	frederico.chaves@tjpi.jus.br	**Telefone**	86 3230-7869
Integrante Administrativo	Giovanny Lima de Castro	**Matrícula**	**28631**
E-mail	giovanny.castro@tjpi.jus.br	**Telefone**	86 3230-7869
Integrante Administrativo	Fábio Rogério Nóbrega Ribeiro	**Matrícula**	30641
E-mail	fabionobregaribeiro@tjpi.jus.br	**Telefone**	86 3230-7869

16. Equipe de gestão da contratação (art. 16, VIII)

Considerando que atualmente fora realizado pela EJUD treinamentos para servidores dos diversos setores no tema de Fiscalização de Contratos, considerando ainda que outras turmas estão previstas, sugerimos que sejam selecionados servidores já capacitados ou com previsão de treinamento nas próximas turmas para comporem a equipe.

Sugerimos ainda, visando atender à segregação de funções, que os designados para a fiscalização sejam servidores que NÃO fazem parte desta equipe de contratação.

ANÁLISE DE RISCOS (art. 17)

17. Riscos do processo de contratação (art. 17, I)

Risco 1 – Restrição orçamentária					
Probabilidade	Impacto	Ação preventiva	Responsável	Ação de contingência	Responsável
Média	Alto	Priorização deste projeto em detrimento de outras iniciativas	Equipe de Planejamento da Contratação	Reduzir a contratação de dois anos para um ano.	Integrante requisitante
Risco 2 – Não cumprimento dos prazos acordados					

Probabilidade	Impacto	Ação preventiva	Responsável	Ação de contingência	Responsável
Média	Alto	Monitorar e notificar preventivamente a contratada para que cumpra os prazos	Fiscal técnico	Propor a aplicação de sanções previstas em contrato	Fiscal demandante

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Chefe de Seção de Aquisições e Contratações de Soluções de TIC**, em 12/04/2023, às 07:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **4190382** e o código CRC **7149E67F**.