



PODER JUDICIÁRIO
JUSTIÇA FEDERAL

TRIBUNAL REGIONAL FEDERAL DA 2ª REGIÃO

MCTI - ESTUDO TÉCNICO PRELIMINAR (ETP) TRF2 0928835

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.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1 Identificação das necessidades de negócio

A	Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal (PETI-JF 2021-2026)
B	Aprimorar a Segurança da Informação e a Gestão de Dados (ENTIC-JUD 2021-2026)
C	Assegurar níveis de serviços adequados ao negócio
D	Garantir confidencialidade e autenticidade nos serviços Web

1.2 Identificação das necessidades tecnológicas

A	Certificados digitais A1 para equipamentos servidores e serviços de rede
B	Certificados digitais emitidos por autoridade certificadora habilitada
C	Certificados digitais reconhecidos pelos navegadores Microsoft Edge, Google Chrome, Mozilla Firefox e Safari
D	Certificados digitais compatíveis com sistemas operacionais Windows, Linux, Android e Apple
E	Certificados digitais compatíveis com os serviços/sistemas Microsoft Exchange, Microsoft IIS, Apache Web Server e JBoss Enterprise

1.3 Demais requisitos necessários e suficientes à escolha da solução de TIC

A	Requisitos legais: Lei 14.133/2021 que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios. Lei 13.709/2018, alterada pela Lei 13.853/2019 - Lei Geral de Proteção de Dados Pessoais (LGPD); Resolução CNJ 396/2021 que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); Resolução CJF 687/2020 que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de 1º e 2º graus; Resolução TRF2-RSP-2023/00043 que trata sobre a Política de Segurança da Informação da Justiça Federal da 2ª Região.
B	Requisitos de manutenção: Os certificados digitais deverão ter mantidas as suas características operacionais durante o período de sua vigência contados logo após a emissão; A Contratada deverá fornecer serviço de suporte técnico durante toda a vigência do Contrato. O suporte técnico poderá ser realizado por telefone, e-mail, abertura de chamados on-line em horário comercial e em língua portuguesa do Brasil; Não poderá existir qualquer limitação de horas para a prestação do serviço de suporte técnico; Certificados digitais revogados por erros identificados nos dados neles contidos deverão ser reemitidos pela Contratada com a correção dos dados, sem ônus adicional; Certificados digitais revogados por motivação exclusiva do Contratante não precisarão ser substituídos a título de garantia.
C	Requisitos temporais: Os serviços de emissão de certificados digitais devem ser iniciados em até 05 (cinco) dias após a assinatura do Contrato; Os certificados digitais emitidos deverão ter garantia de 12 (doze) meses contados a partir da data de emissão de cada certificado; O atendimento para chamados de suporte técnico poderá ser realizado em dias úteis no horário entre 08:00 h e 18:00 h, durante a vigência da validade de cada certificado emitido.
D	Requisitos de capacitação: Deverão ser fornecidas documentações e orientações com instruções para requisição, emissão e instalação dos certificados digitais.
E	Requisitos de segurança: Observação rigorosa de todas as normas e procedimentos de segurança adotados no ambiente do Contratante; São vedadas a divulgação, a reprodução ou a utilização de quaisquer informações, a qualquer título, exceto quando previamente autorizadas; São vedadas a cópia, reprodução, divulgação ou a utilização de quaisquer conteúdos de manuais, documentações ou processos administrativos e judiciais, a qualquer título, exceto quando previamente autorizadas; Seguir as recomendações de segurança da informação da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).
F	Requisitos ambientais: Não há impactos ambientais a serem mitigados, tendo em vista que os trâmites da contratação serão realizados de forma eletrônica, sem confecção e transporte de mídias ou papel e, além disso, a solicitação e emissão dos certificados digitais serão feitas todas de forma "on-line".

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Descrição	Quantidade total a ser adquirida
Emissão de certificados A1 do tipo Wildcard SSL internacional (múltiplos domínios) para equipamentos servidores	35
Emissão de certificados A1 do tipo SSL internacional (único domínio) para equipamentos servidores	52
Emissão de certificados A1 do tipo SAN SSL internacional com até 05 nomes adicionais para equipamentos servidores	24

A aquisição de certificados digitais para equipamentos servidores destina-se especificamente ao atendimento das demandas do Contratante que envolve a proteção de sistemas Web disponibilizados via Internet.

O quantitativo apresentado advém do número de domínios/subdomínios que precisam de certificado e o tipo de cada certificado que pode ser Wildcard SSL internacional, SSL internacional ou SAN SSL internacional. Para o cálculo do quantitativo também foi levado em consideração a eventual necessidade de certificados adicionais para atendimento de novos domínios durante a vigência do Contrato.

O número total de cada tipo de certificado foi calculado com base nas demandas sinalizadas pelos órgãos conforme abaixo:

- TRF2: 03 certificados Wildcard, 02 SSL e 02 SAN;
- JFRJ: 03 certificados Wildcard, 02 SSL e 02 SAN;
- JFES: 02 certificados Wildcard e 24 SSL;
- TRF5: 10 certificados Wildcard, 10 SSL e 04 SAN;
- JFCE: 04 certificados Wildcard e 06 SAN;
- JFPE: 01 certificado Wildcard, 02 SSL e 02 SAN;
- JFRN: 10 certificados Wildcard, 10 SSL e 06 SAN;
- JFSE: 02 certificados Wildcard, 02 SSL e 02 SAN;

3. ANÁLISE DE SOLUÇÕES POSSÍVEIS	
3.1 Identificação das soluções	
Ao realizar a análise do mercado de TI foram encontradas as seguintes alternativas:	
Id	Descrição da solução (ou cenário)
01	Emissão de certificados digitais gratuitos
02	Emissão de certificados digitais pagos

3.2 Análise comparativa das soluções		
Para a alternativa 01 foi identificada a solução de emissão de certificados digitais da Let's Encrypt (https://letsencrypt.org) que é uma certificadora patrocinada por várias empresas de tecnologia como a IBM, Google e Cisco, entre outras. A proposta da Let's Encrypt é emitir certificados digitais para equipamentos de maneira gratuita utilizando mecanismos de automação, reduzindo custos e facilitando o processo como um todo. Os certificados da Let's Encrypt possuem validade máxima de 90 (noventa) dias o que implica em renovar os certificados logo após esse prazo. Além disso, não são oferecidos serviços de suporte dedicado para solução de problemas na emissão ou na instalação dos certificados. Já para a alternativa 02, existem diversas empresas no mercado habilitadas como autoridades certificadoras capazes de fornecer certificados digitais com validade de, pelo menos, 01 (um) ano. Além da emissão, essas empresas incluem serviços de suporte dedicado para solução de problemas na geração ou na instalação dos certificados, durante todo o período de validade dos mesmos. Observou-se que na alternativa 01 o prazo de 90 (noventa) dias de validade dos certificados é relativamente curto comparado com o prazo de 01 (um) ano da alternativa 02. Isso eleva o risco de interrupção dos serviços por falha no processo de renovação dos certificados ou por indisponibilidade da Let's Encrypt. A falta de um serviço de suporte dedicado para solução de problemas também pode acarretar em falhas que podem comprometer os serviços Web que dependem dos certificados digitais, comprometendo a confidencialidade, autenticidade e a disponibilidade. Portanto, a alternativa 01 foi descartada sendo escolhida a alternativa 02 “Emissão de certificados digitais pagos”.		
A tabela abaixo mostra uma análise comparativa entre as soluções identificadas quanto a alguns requisitos:		
Requisito	Solução 01	Solução 02
Certificados digitais A1 para equipamentos servidores e serviços de rede	SIM	SIM
Certificados digitais emitidos por autoridade certificadora habilitada	SIM	SIM
Certificados digitais reconhecidos pelos navegadores Microsoft Edge, Google Chrome, Mozilla Firefox e Safari	SIM	SIM
Certificados digitais compatíveis com sistemas operacionais Windows, Linux, Android e Apple	SIM	SIM
Certificados digitais compatíveis com os serviços/sistemas Microsoft Exchange, Microsoft IIS, Apache Web Server e JBoss Enterprise	SIM	SIM
Os certificados digitais emitidos com garantia de 12 (doze) meses contados a partir da data de emissão de cada certificado	NÃO	SIM
Atendimento de suporte técnico durante a vigência da validade de cada certificado emitido	NÃO	SIM

A tabela abaixo mostra a comparação de custos entre as soluções identificadas:						
Id	Descrição	Preço 1	Preço 2	Preço 3	Média	Observação
01	Emissão de certificados digitais gratuitos	N/A	N/A	N/A	N/A	Não se aplica, pois não existem custos para emissão de certificados gratuitos via Let's Encrypt
02	Emissão de certificados digitais pagos	R\$ 2199,00	R\$ 2301,20	R\$ 1890,00	R\$ 2130,06	Preço 1: https://certisign.com.br Preço 2: https://www.soluti.com.br Preço 3: https://www.sectigo.com.br

O quadro abaixo apresenta a utilização e a aderência das soluções quanto a determinadas políticas, modelos e padrões de governo existentes:

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	01	X		
	02	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	01			X
	02			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	01			X
	02			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	01			X
	02			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	01	X		
	02	X		
A Solução é aderente às orientações, premissas e especificações do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	01			X
	02			X

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

A solução 01 (Emissão de certificados digitais gratuitos) foi considerada inviável, pois, só permite a emissão de certificados com prazo máximo de 90 (noventa) dias o que pode prejudicar a segurança das aplicações Web, caso não seja possível renovar em função do prazo curto ou de indisponibilidade da Let’s Encrypt. Além disso, essa solução não possui serviço de suporte técnico para solução de problemas o que também é necessário para garantir a resolução de problemas que podem impactar no uso dos certificados e, consequentemente, colocar em risco as aplicações que deles dependem.

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO) DAS SOLUÇÕES TÉCNICA E FUNCIONALMENTE VIÁVEIS

5.1 Cálculos dos custos totais de propriedade

Não foram realizados cálculos de custos totais de propriedade tendo em vista que só existe uma solução técnica e funcionalmente viável o que tornaria sem sentido uma análise comparativa.

6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A solução a ser contratada tem a finalidade de garantir todos os requisitos e etapas necessárias para o processo de emissão de certificados digitais por autoridade certificadora autorizada que permita criptografia, confidencialidade e autenticidade nos serviços Web oferecidos pelos Órgãos via Internet.

Além da emissão, a solução deve contemplar serviços de garantia e suporte durante todo o período de validade dos certificados emitidos de forma a solucionar problemas e corrigir erros, evitando a interrupção dos processos de negócio que dependem da solução em si.

Características gerais da solução:

- Fornecer certificados digitais formato A1 para equipamentos servidores;
- Possuir validade de 12 (doze) meses para os certificados, contados a partir da data de emissão, de acordo com o tipo e formato do certificado;
- Ser reconhecido nos navegadores Microsoft Edge, Google Chrome e Mozilla Firefox e Safari;
- Ser compatível com os sistemas operacionais Windows, Linux, Android e Apple;
- Ser compatível com os serviços/sistemas Microsoft Exchange, Microsoft IIS, Apache Web Server e JBoss Enterprise;
- Incluir serviço de suporte técnico sem limitação de quantidade de horas ou chamados;

Permitir a substituição/reemissão de certificados revogados com ou sem ônus de acordo com a causa.

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO DA SOLUÇÃO ESCOLHIDA

O custo total da contratação está estimado em R\$ 55.157,98 (Cinquenta e cinco mil, cento e cinquenta e sete Reais e noventa e oito centavos).

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente Estudo Técnico Preliminar está de acordo com as necessidades técnicas e operacionais do Órgão. Também está consoante com o objetivo estratégico "Aperfeiçoar e Assegurar efetividade dos serviços de TI para a Justiça Federal" do Plano Estratégico de TI da Justiça Federal (PETI-JF) 2021-2026, bem como o objetivo "Aprimorar a Segurança da Informação e a Gestão de Dados" que consta no ENTIC-JUD conforme Resolução nº 370/2021 alterada pela Resolução nº 396/2021 do CNJ.

Durante a elaboração do Estudo foram levadas em consideração as necessidades de negócio que dependem intrinsecamente dos sistemas Web expostos via Internet e que precisam garantir autenticidade, confidencialidade e disponibilidade.

A alternativa escolhida na fase de Análise de Soluções Possíveis foi a que se mostrou viável e exequível do ponto de vista técnico e que melhor atende aos principais requisitos de negócio enquanto a Pesquisa de Preços de Mercado demonstrou que a alternativa possui custos adequados à disponibilidade orçamentária.

Os quantitativos levantados na Estimativa da Demanda foram calculados de forma a atender todos os domínios sobre os quais as aplicações Web são disponibilizadas, bem como também prevendo futuras aplicações que venham a necessitar dos mesmos mecanismos de segurança providos pelos certificados.

Assim sendo, a Equipe de Planejamento da Contratação entende que o presente Estudo está de acordo com as necessidades do Órgão, que é justificadamente viável quanto aos requisitos de negócios, administrativos e técnicos a serem alcançados, declarando viável a aquisição proposta.

9. DA APROVAÇÃO DO ETP E ASSINATURA			
A Equipe de Planejamento da Contratação foi instituída pela Portaria SEI DG/TRF2 Nº 47, de 04 de fevereiro de 2025.			
Conforme o § 2º do Art. 11 da IN SGD/ME nº 94 de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Demandantes e pela autoridade máxima da área de TIC.			
PAPEL	NOME	MATRÍCULA	SETOR
Integrante Requisitante (titular):	Marcus Vinícius do P. Azevedo	T211728	DIREM
Integrante Requisitante (suplente):	Pergentino Joaquim Alves Neto	T212049	SITI
Integrante Técnico (titular):	Samir Gerard D’Angelis Chalhoub	T211739	DIREM
Integrante Técnico (suplente):	Pergentino Joaquim Alves Neto	T212049	SITI
Integrante Administrativo (titular):	Gabriel de Farias Antunes	T211833	DIMAT
Integrante Administrativo (suplente):	Leonardo Pastro Vieira	T211795	DIMAT



Documento assinado eletronicamente por **MARCUS VINICIUS DO PATROCINIO AZEVEDO**, **Diretor**, em 28/04/2025, às 12:54, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SAMIR GERARD D'ANGELIS CHALHOUB**, **Técnico Judiciário**, em 28/04/2025, às 13:14, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **GABRIEL DE FARIAS ANTUNES**, **Técnico Judiciário**, em 29/04/2025, às 18:18, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.trf2.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0928835** e o código CRC **C447687A**.