

ESTUDOS TÉCNICOS

1. INTRODUÇÃO

1.1. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de Certificados Digitais bem como fornecer informações necessárias para subsidiar o respectivo processo.

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

2.1. Emissão de Certificados Digitais com Token, sem Token, armazenamento em nuvens, certificados para domínio e para servidores.

2.2. Esta solução consiste em um conjunto integrado de formas de armazenamento de certificados digitais, em tokens ou em nuvem que possibilitem o trabalho de implantação do Processo Judicial Eletrônico(PJE), tanto nas zonas eleitorais como na sede, bem como acesso aos demais sítios que necessitam de validação eletrônica através de certificados digitais.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES

3.1. Necessidades de Negócio da Unidade Requisitante

3.1.1. Garantir a autenticidade e a integridade nas transações eletrônicas de pessoas físicas, tendo validade jurídica para ser utilizado como assinatura de próprio punho, comprovando que seu proprietário concorda com o documento assinado;

3.1.2. O tipo de certificado digital a ser escolhido depende do sistema/aplicação no qual será utilizado. O sistema PJE requer certificados do tipo A3, por oferecerem maior mobilidade e segurança, uma vez que emitidos em mídia criptográfica;

3.1.3. É requerido esse padrão nacional oficial para os certificados digitais a serem utilizados no sistema PJE;

- 3.1.4. Propiciar maior vantagem econômica na contratação (em vista do melhor custo relativo dos valores ofertados para as emissões de certificados com validade de 36 meses em relação aos emitidos com validade de 12 meses), bem como maior satisfação aos usuários devido à dispensa de validações anuais;
- 3.1.5. Manter padronização já existente no TRE/CE, com a utilização de TOKEN com entrada USB e reduzir custos com novos certificados em nuvem.
- 3.1.6. Aumentar a colaboração e comunicação corporativa, promovendo dessa forma maior engajamento e produtividade nas unidades de trabalho do Tribunal Regional Eleitoral do Ceará;

3.2. Demais Requisitos

3.2.1. Repasse de conhecimento:

3.2.1.1. Garantir a autenticidade e a integridade nas transações eletrônicas de pessoas físicas, tendo validade jurídica para ser utilizado como assinatura de próprio punho, comprovando que seu proprietário concorda com o documento assinado.

3.2.1.2. O tipo de certificado digital a ser escolhido depende do sistema/aplicação no qual será utilizado. O sistema PJE requer certificados do tipo A3, por oferecerem maior mobilidade e segurança, uma vez que emitidos em mídia criptográfica;

3.2.1.3. É requerido esse padrão nacional oficial para os certificados digitais a serem utilizados no sistema PJE;

3.2.2. Manutenção e Suporte:

3.2.2.1 A contratada deverá prestar suporte técnico em horário comercial no regime de atendimento remoto, por telefone (em português) e/ou por e-mail, para a solicitação, instalação e utilização do certificado digital;

3.2.2.2 A contratada deverá disponibilizar página na internet para ativação, manutenção, emissão ou substituição do certificado durante a validade da sua emissão;

3.2.2.3 Disponibilizar, em regime 24 horas por dia, 7 dias por semana, página na internet para download do certificado assinado;

3.2.2.4 Prover garantia de correção e atualização motivadas por falhas técnicas e mudanças originadas de diretrizes oriundas da ICP-Brasil, pelo período mínimo de 1 (um) ano para o objeto em questão, contados a partir da data de emissão do certificado;

3.2.2.5 Caso ocorram falhas, necessidades de correção ou atualização que exija novo certificado, a empresa contratada deverá efetuar a nova emissão no prazo máximo de 5 (cinco) dias corridos, contados da data de notificação, sem ônus adicional para este Tribunal;

3.3. LEVANTAMENTO DAS ALTERNATIVAS

3.3.1 As possíveis alternativas para atender à nossa solução passam por três soluções:

3.3.1.1 O primeiro: a solução Certificados Cert-JUS tipo A3 com Token - 36 meses, onde os certificados digitais são instalados nos dispositivos físicos conhecidos como tokens;

3.3.1.2 O segundo: a solução Certificados Cert-JUS tipo A3 sem Token- 36 meses onde os certificados digitais serão instalados em tokens da marca GD STARSING BURTI, já em uso neste Tribunal;

3.3.1.3 O terceiro: a solução Certificados Cert-JUS tipo A3 em nuvem - 36 meses, referência NeoID, modelo utiliza o paradigma em nuvem onde toda a responsabilidade fica a cargo do fornecedor, implicando em uma alternativa muito mais vantajosa para a administração.

3.3.2. O Custo da solução Certificados Cert-JUS tipo A3 com Token - 36 meses foi orçado em R\$ 128.500,00 para 300 usuários.

3.3.2.1 Fornecedor: Certisign, valor unitário R\$ 418,00, link de acesso: <https://www.certisign.com.br/certificado-digital/ecpf>

3.3.2.2 Fornecedor: Serasa Experian, valor unitário R\$ 404,00, link de acesso: <https://compra.certificadodigital.com.br/loja/#!/identificacao/e-CPF/0646/e-CPF-A3-36-MESES-TOKEN>

3.3.2.3 Fornecedor: Valid Certificadora, valor unitário R\$ 463,00, link de acesso: <https://www.validcertificadora.com.br/e-CPF-A3-de-3-anos-em-token.htm>

3.3.2.4. Análise da Solução: Solução bastante completa e padrão dentro dos fornecimentos concernentes a emissão de certificados digitais permitindo uma melhor desempenho, segurança e integridade entre o hardware e o software apresentado. Apontando para a forma tradicional de expedição de certificados dessa natureza.

3.3.3. O Custo da solução Certificados Cert-JUS tipo A3 sem Token - 36 meses foi orçado em R\$ 24.336,67 (Vinte e quatro mil e trezentos e trinta e três reais e sessenta e sete centavos) para 100 usuários.

3.3.3.1 Fornecedor: Certisign, valor unitário R\$ 224,00, link de acesso: <https://www.certisign.com.br/certificado-digital/ecpf>

3.3.3.2 Fornecedor: Serasa Experian, valor unitário estimado em R\$ 244,00, link de acesso: <https://compra.certificadodigital.com.br/loja/#!/identificacao/e-CPF/0646/e-CPF-A3-36-MESES-TOKEN>

3.3.3.3 Fornecedor: Valid Certificadora, valor unitário R\$ 263,00 link de acesso: <https://www.validcertificadora.com.br/ComprePorProduto.aspx?nome=e-CPF>

3.3.3.4. Analise da Solução: Solução bastante completa e padrão dentro dos fornecimentos concernentes a emissão de certificados digitais permitindo uma melhor desempenho, segurança e integridade entre o hardware e o software apresentado. Apontando para a forma tradicional de expedição de certificados dessa natureza.

3.3.4. O Custo da solução Certificados Cert-JUS tipo A3 em nuvem - 36 meses foi orçado em R\$ 35.990,00 para 150 usuários

3.3.4.1 Fornecedor: Certisign, valor unitário R\$ 390,00, link de acesso: <https://www.certisign.com.br/certificado-digital/ecpf>

3.3.4.2 Fornecedor: SERPRO, valor unitário R\$ 179,90, link de acesso: <https://servicos.serpro.gov.br/neoid/#comprar>

3.3.4.3 Analise da Solução: Solução bastante completa e padrão dentro dos fornecimentos concernentes a emissão de certificados digitais permitindo uma melhor desempenho, segurança e integridade entre o hardware e o software apresentado. Apontando para a forma tradicional de expedição de certificados dessa natureza.

3.6. Cenário Escolhido

3.6.1. Dentre o levantamento apresentado, o mais viável será aquele que atender aos princípios da viabilidade técnica respeitado a economicidade para um conjunto de 300(trezentos) Certificados Cert-JUS tipo A3 com Token, 100 (cem) Certificados Cert-JUS tipo A3 sem Token e 150 (cento e cinquenta) Certificados Cert-JUS tipo A3 em Nuvem.

3.6.2. Para que não haja prejuízo de fornecimento e zelando pela oportunidade de qualquer empresa participar sugerimos que poderá ser fornecido o serviço por duas empresas desde que seja garantido o fornecimento dos Certificados Cert-JUS tipo A3 com token e sem token seja contemplado pela mesma empresa. De forma a

não inviabilizar o uso de certificados digitais Cert-JUS tipo A3 em nuvem poderá ser oferecido por uma outra empresa.

3.6.3. Os fornecimentos dos itens Certificados Cert-JUs Tipo A3 sem token devem contemplar a compatibilidade com os tokens GD STARSING BURTI salientando que os os modelos dos tokens utilizados pelos usuários são baseados nesse padrão de forma a garantir a continuidade dos serviços de acesso e armazenamento do certificado neste tipo de armazenamento móvel.

3.7. Justificativa do Cenário Escolhido

3.7.1. Optamos pela Configuração de diversificar o tipo da compra de certificados com token, sem token e em nuvem, por:

3.7.1.1. Para os certificados com tokens teremos a possibilidade de atender as novas demandas de primeira solicitação de usuário que necessitará de tokens e certificados;

3.7.1.2. Para os certificados sem tokens teremos a possibilidade de atender as demandas de usuários que já possuem certificados digitais com tokens e por ventura precisem de nova emissão;

3.7.1.3. Para certificados em Nuvem trata-se de uma nova proposta de tecnologia que permite o usuário final a utilizar a validação do certificado em nuvem de maneira a não necessitar do dispositivo de armazenamento para guarda do certificado digital. Por se tratar de tecnologia nova será avaliado a sua utilização e viabilidade com a possibilidade migrar todos os certificados para essa modalidade de validação sem a necessidade do meio físico para armazenamento.

3.8. Bens e Serviços que compõem a solução escolhida

id	Descrição	Quantidade
1	Certificados Cert-JUS tipo e-CPF A3 com Token	300
2	Certificados Cert-JUS tipo e-CPF A3 sem Token	100
3	Certificados Cert-JUS tipo e-CPF A3 em nuvem	150
4	Certificados Cert-JUS tipo e-CNPJ A1	4
5	Certificados Cert-JUS tipo e-CNPJ A3	4
6	Certificados Site Seguro SSL Wildcard	1

	Visitas técnicas para emissões	30
	Total	585

3.9. Alinhamento em relação as necessidades de negócio e macro requisitos tecnológicos

3.9.1. Atualmente o TRE-CE possui 1.813 (Um mil e oitocentos e treze) servidores, de acordo com o último questionário informativo do iGovTI, com possibilidade de atuarem frente ao uso de certificados digitais sendo que atualmente.

3.10. Benefícios a serem alcançados

3.10.1. Alinhamento Estratégico:

3.10.1.1. PETIC, OBJETIVO ESTRATÉGICO 5: PROMOVER A MODERNIZAÇÃO E PADRONIZAÇÃO TECNOLÓGICA

3.10.2. Metas do Planejamento Estratégico a serem Alcançadas:

3.10.2.1. Índice de aderência a infraestrutura da ENTIC-JUD

3.10.3 Oferecer garantia para os usuários dos serviços do Tribunal que os serviços são confiáveis e legítimos;

3.10.4 manter em níveis adequados a segurança no tráfego das informações fornecidas pelos sistemas eletrônicos que necessitam de validação e autenticação através de certificados digitais;

3.10.5 garantir que os dados sensíveis dos serviços do Tribunal trafeguem com segurança sob criptografia forte.

5. RECURSOS NECESSÁRIOS À IMPLANTAÇÃO E À MANUTENÇÃO DA SOLUÇÃO

5.1. Recursos Legais:

5.1.1 Para elaboração deste Termo de Referência foram observadas, entre outras normas:

5.1.1.1 Lei Federal nº 8.666/1993: Institui normas para licitações e contratos da Administração Pública e dá outras providências;

5.1.1.2 Lei Federal nº 10.520/2002: Institui no âmbito da União, Estados, Distrito Federal e Municípios, a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

5.1.1.3 Decreto nº 3.996/2001: Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;

5.1.1.4 Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

5.1.1.5 Decreto nº 5.450/2005: Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;

5.1.1.6 Instrução Normativa SLTI-MPOG nº 04/2014: Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.

6. ESTRATÉGIA DE CONTINUIDADE DA SOLUÇÃO EM CASO DE INTERRUPÇÃO CONTRATUAL

6.1. Descrição do Evento

6.1.1. Ação Preventiva: A empresa contratada deverá fornecer acesso por pelo menos 180 (cento e oitenta) dias para transferir os dados ora armazenados, tais como relatórios de certificados emitidos e todas as informações pertinentes a emissão como data de expiração e validade dos certificados.

6.1.2. Responsáveis pela ação preventiva: Empresa contratada e Secretaria de Tecnologia da Informação.

6.1.3. Ação de Contingência: Disponibilizar acesso em mais de um site.

6.1.4. Responsáveis pela ação de contingência: Empresa contratada.

7. ADEQUAÇÃO ORÇAMENTÁRIA

7.1. Fonte de Recursos:

7.1.1. A adequação orçamentária será realizada por Unidade competente da Secretaria de Administração e Orçamento e será inserido no processo de contratação previamente à aprovação do Edital.

7.2. Orçamento detalhado

id	Descrição	Quantidade	Unidade	Valor unitário estimado (R\$)	Valor total estimado (R\$)
1					

2					
3					
4					
5					

7.3. Estimativa de Impacto econômico-financeiro

id	Exercício	Percentual	Análise e Conclusão
1			
2			
3			
4			
5			

7.4. Cronograma de execução físico-financeira

id	Entrega	Data	Percentual
1			
2			
3			
4			
5			

8. ADERÊNCIA DA SOLUÇÃO

Requisito	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	X		
A Solução é um software livre ou software público?		X	
A Solução está disponível no Portal do Software Público Brasileiro?		X	
A Solução está disponível em outros Órgãos ou entidades da Administração Pública?	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelo Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	X		
A Solução é aderente às regulamentações da ICP-Brasil? (Quando houver necessidade de certificação 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 Poder Judiciário (Moreq-Jus)?			

9. ESTRATÉGIA DA CONTRATAÇÃO

Critério	Atendimento da solução
É possível especificar o serviço usando parâmetros usuais de mercado?	Sim
É possível medir o desempenho da qualidade usando Parâmetros usuais de mercado?	Sim
O objeto da contratação se estende necessariamente por mais de um ano?	Sim
O objeto da contratação é essencial para o negócio?	Sim

9.1. Recursos necessários à continuidade do negócio durante e após a execução do contrato

9.1.1. Será de responsabilidade dos Gestores técnicos e demandantes a gestão e operação deste contrato.

9.2. Estratégia de continuidade contratual

9.2.1. Havendo qualquer evento de inexecução contratual, que acarrete no distrato ou encerramento contratual, os serviços serão suspensos, e será avaliada a possibilidade de nova contratação sem prejuízo da aplicação das penalidades previstas.

9.3. Estratégia de transição e encerramento do contrato

9.3.1. Por tratar-se de serviço continuado, o contrato terá vigência de 12 (dose) meses, podendo ser renovado, por iguais e sucessivos períodos até o limite previsto na legislação vigente.

9.3.2. Havendo necessidade, a nova contratação deverá ser iniciada com 120 dias de antecedência, sendo de responsabilidade do Secretário de Tecnologia da Informação.

9.4. Estratégia de independência

9.4.1. Transferência de Conhecimento: Por tratar-se de serviço, emissão de certificados e alimentação de dados, com a finalidade de garantir a atualização e o funcionamento dos certificados digitais, será prevista a prorrogação contratual para os serviços de subscrição.

9.4.2. Havendo necessidade, a nova contratação deverá ser iniciada com 120 dias de antecedência, sendo de responsabilidade do Secretário de Tecnologia da Informação.

10. ANÁLISE DE RISCOS

10.1. A Análise de Riscos irá descrever e avaliar as ameaças que possam vir a comprometer o sucesso e o objetivo da contratação, bem como definir de que formas devem ser tratadas, ela permeará todo processo de Contratação.

10.2. Riscos do processo de contratação

10.2.1. Descrição detalhada do Risco: Estabelecimento de requisitos desconectados da necessidade da contratação.

10.2.1.1. Fator de Risco (Causa): Falta de conhecimento da equipe de contratação.

10.2.1.2. Severidade inerente: Alta

10.2.1.3. Descrição do Controle: Buscar levantar todas as necessidades e soluções disponíveis.

10.2.1.4. Responsável pelo Controle: COINT(Coordenadoria de Infraestrutura Tecnológica)

10.2.1.5. Severidade residual: Baixa

10.2.1.6. Ação de Contingência: não há

10.2.1.7. Responsável pela Contingência: não se aplica

10.2.2. Descrição detalhada do Risco: Adoção de tipo de solução imaturo, levando a problemas na implantação ou descontinuidade da solução antes do órgão conseguir desfrutar do investimento feito na solução

10.2.2.1. Fator de Risco (Causa): Escolha de solução com pouco uso no mercado.

10.2.2.2. Severidade inerente: Alta

10.2.2.3. Descrição do Controle: Levantar soluções com pelo menos 01 (um) ano de maturidade.

10.2.2.4. Responsável pelo Controle: COINT(Coordenadoria de Infraestrutura Tecnológica)

10.2.2.5. Severidade residual: Baixa

10.2.2.6. Ação de Contingência: não há

10.2.2.7. Responsável pela Contingência: não se aplica

10.2.3. Descrição detalhada do Risco: A solução contratada ser incompleta, de forma a não atender à necessidade da contratação.

10.2.3.1. Fator de Risco (Causa): Estudo técnico não aprofundado.

10.2.3.2. Severidade inerente: Alta

10.2.3.3. Descrição do Controle: Checar se a solução atende aos requisitos levantados.

10.2.3.4. Responsável pelo Controle: Equipe de contratação

10.2.3.5. Severidade residual: Baixa

10.2.3.6. Ação de Contingência: não há

10.2.3.7. Responsável pela Contingência: não se aplica

10.2.4. Descrição detalhada do Risco: Interrupção Contratual por qualquer motivo

- 10.2.4.1. Fator de Risco (Causa): Ruptura contratual de qualquer natureza
- 10.2.4.2. Severidade inerente: Alto
- 10.2.4.3. Descrição do Controle: Manter estratégia de transição de plataforma atualizada e com verificação mensal.
- 10.2.4.4. Responsável pelo Controle: COINT(Coordenadoria de Infraestrutura Tecnológica)
- 10.2.4.5. Severidade residual: Baixa
- 10.2.4.6. Ação de Contingência: Acompanhar o processo de emissão junto ao usuários até sua finalização caso a caso.
- 10.2.4.7. Responsável pela Contingência: STI (Secretaria de Tecnologia da Informação)

11. DECLARAÇÃO DE VIABILIDADE

11.1. Com base nas informações levantadas neste estudo, a equipe de planejamento declara que a contratação de Certificados Digitais é viável, encaminhando à Diretoria-Geral para conhecimento e providências.