



MINISTÉRIO DAS COMUNICAÇÕES

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

(Contratação por Dispensa de licitação, Inexigibilidade e modalidades tradicionais)

INTRODUÇÃO

O Estudo Técnico Preliminar da Contratação é o documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação.

Este documento deverá ser elaborado de acordo com o Art. 11 da Instrução Normativa nº 01, de 04 de abril de 2019, emitida pela Secretaria de Governo Digital do Ministério da Economia (IN SGD nº 01/2019).

1 - Objetivo

Estudo Técnico Preliminar da Contratação é documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação e integra a fase de Planejamento da Contratação de Soluções de Tecnologia da Informação e Comunicação – conforme regulamentado pela Instrução Normativa nº 01, de 04 de abril de 2019, da Secretaria de Governo Digital do Ministério da Economia.

2 - NECESSIDADE DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Certificados Digitais A1

Com a evolução dos sistemas em meio digital tornou-se preponderante implementar uma forma de garantir a integridade, confiabilidade e autenticidade das informações em meios tecnológicos

A tecnologia atual, capaz de prover tais características, é a certificação digital, um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também validade jurídica de documentos e informações em meios eletrônicos;

O certificado digital funciona como identidade virtual, permitindo a identificação segura e inequívoca do usuário, de uma mensagem ou transação em meio eletrônico. No tocante ao certificado de equipamento garante com a mesma segurança a identificação de servidores Web (SSL) e Aplicações;

No Brasil, foi estabelecido pela Medida Provisória nº 2.202-2, de 24 de agosto de 2001, a ICP-Brasil, gerida pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil), que atua na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil, inclusive nos aspectos de normalização e nos procedimentos administrativos, técnicos, jurídicos e de segurança, que forma a cadeia de confiança da ICP-Brasil;

A tecnologia do “webservice” possibilita a integração entre diferentes sistemas, proporcionando a interação máquina-máquina através da rede de computadores. Esta tecnologia permitiu que sistemas desenvolvidos em linguagens e plataformas diferentes realizem a troca de dados no mesmo formato;
Entre os certificados digitais do tipo A1 a serem adquiridos, um deles será utilizado para possibilitar a disponibilização de sistemas e portais do Ministério, como por exemplo o SEI.

Certificado Digital A3

Os certificados digitais para pessoa física são utilizados pelos usuários do MCOM para acesso aos diversos sistemas entre eles: Comprasnet, SIAFI, SIGEPE e outros. Os Certificados Digitais A3 pessoa física tem validade de 3 anos.

Embora exista no mercado a oferta de certificados digitais de padrões internacionais, a APF somente poderá adquirir certificados emitidos pela autoridade certificadora ICP Brasil, conforme decreto presidencial nº DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001, que dentre outros diz o seguinte: "Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil". Logo, apenas certificados deste tipo poderão ser considerados.

Token (mídia criptográfica)

Diante o exposto, a aquisição pretendida justifica-se, pela necessidade de substituição dos Tokens perdidos, danificados, expirados e em vias de vencimento, atualmente em utilização no MCOM, além de novos tokens destinados aos servidores da casa.

Certificado em nuvem (NEOID)

O Certificado Digital, conhecido por viabilizar transações no meio eletrônico com validade jurídica e total segurança, agora, também pode ser armazenado na nuvem e com validade de até cinco anos. Sua emissão pode ser realizada por todas as Autoridades Certificadoras credenciadas pelo Instituto Nacional de Tecnologia da Informação (ITI) e autorizadas a emitir o Certificado neste formato.

No âmbito dos órgãos e entidades da Administração Pública Federal uma das facilidades adicionais desse formato é a possibilidade de utilização do Sistema de Gestão de Pessoal (SIGEPE), do Ministério da Economia, para realização da validação do registro de forma individualizada e totalmente eletrônica para os servidores públicos federais, dispensando a fase de validação presencial – conforme definido na Instrução Normativa nº 6, de 11 de agosto de 2017, do Instituto Nacional de Tecnologia da Informação¹.

Tal alternativa tem o objetivo de reduzir o custo de emissão do certificado digital (CD) com outras ARs, dar maior mobilidade aos usuários, prover uma massificação do uso da solução sem a necessidade de tokens físicos e ampliação do acesso do cidadão aos serviços do Governo Federal, com possibilidade de expansão de novos serviços com o uso da segurança da informação provida pela solução.

Nesse sentido o Serviço Federal de Processamento de Dados – SERPRO, autoridade certificadora autorizada pelo ITI, já desenvolveu solução de certificação em nuvem totalmente integrada com o SIGEPE – cujo serviço foi denominado como NEOID. Esse projeto de certificação digital de servidores públicos em questão vem sendo desenvolvido com a participação da Secretaria de Governo Digital - SGD e da Secretaria de Gestão – SEGES.

Dentre as principais características do formato de certificação NEOID, que correspondem às necessidades de negócio da solução para o MCOM, podemos listar:

- a) Disponibilidade do certificado NeolD no regime 24x7, com formato de armazenamento em nuvem;
- b) Validade mínima de 3 anos, não requerendo revalidação durante sua vida útil;
- c) Utilização de fluxo direto do Sistema SIGEP para solicitação e autorização de emissão do certificado, onde a chefia é responsável por autorizar a emissão para seus subordinados;
- d) Permissão de revogação de certificados;
- e) Gestão de faturamento com periodicidade mensal, a partir do quantitativo de certificados efetivamente emitidos no mês de referência; e

4 - ALINHAMENTO COM AS ESTRATÉGIAS ORGANIZACIONAIS

Além de estar prevista no Plano Anual de Contratações (PAC), a pretensão também está listada no Plano Diretor de Tecnologia da Informação e Comunicação do Ministério das Comunicações (PDTIC 2020-2021), vinculada à seguinte necessidade priorizada

| DESCRIÇÃO | FONTE |
|---|-------|
| N3 - Provisão, manutenção e atualização do parque de equipamentos e infraestrutura de redes | PDTIC |
| M4 - Prover equipamentos e serviços de infraestrutura | |

5 - DEFINIÇÃO DAS NECESSIDADES

Certificado Digital A3 em nuvem do tipo NEOID, gerenciada pelo sistema SIGEPE.

1. O certificado NeolD deve ser compatível com dispositivos móveis, desktops e notebooks.
2. O certificado NeolD deve permitir aos usuários o acesso ao sistema Sapiens a partir das credenciais do certificado.
3. O certificado NeolD deve permitir aos usuários do sistema Sapiens assinarem documentos digitais (documentos Sapiens).
4. O certificado NeolD não deve requerer do usuário o uso de qualquer tipo de hardware complementar (pen drive, token, etc).
5. Ter validade de 3 anos
6. Ser acessível mediante qualquer tipo de acesso à internet

Certificado Digital e-CPF A3

O certificado digital para pessoas físicas (e-CPF) é utilizado para validação eletrônica de identidade e assinatura de documentos, deve ter validade mínima de 3 anos (36 meses) e ser homologado pela ICP-Brasil.

É comercializado sem o fornecimento de mídia criptográfica de armazenamento e sem mídia criptográfica de armazenamento.

Para os certificados emitidos com a mídia criptográfica, esse dispositivo deverá ser fornecido pela Autoridade de Registro.

Token criptográfico

Os tokens criptográficos utilizados para armazenamento de certificados digitais devem, em geral, atender aos seguintes requisitos:

1. O dispositivo deverá ser obrigatoriamente homologado no âmbito da ICP-BRASIL, conforme previsto nos documentos: DOC-ICP-10, DOCICP-10.01, DOC-ICP-10.02 e DOC-ICP-10.03.
2. O dispositivo deverá estar de acordo com o Programa de Avaliação da Conformidade (PAC) para equipamentos de certificação digital padrão ICP-Brasil, conforme INSTRUÇÃO NORMATIVA 01, de 24 de março de 2015.
3. Possuir indicador luminoso de estado do dispositivo.
4. Possuir conector USB (Universal Serial Bus) tipo A, versão 2.0 ou superior, através de conexão direta a porta, sem necessidade de interface intermediária para leitura.
5. Possuir capacidade mínima de 32 Kbytes para o armazenamento de certificados e chaves públicas e privadas.
6. Suporte a algoritmos e tamanhos de chaves conforme definidos no documento Padrões e Algoritmos Criptográficos da ICP-Brasil - DOC ICP-01.01.
7. Permitir a gravação de chaves privadas e certificados digitais que utilizem os padrões homologados e emitidos pela Autoridade Certificadora.
8. Possuir software de gerenciamento do dispositivo no idioma português que permita, no mínimo, as seguintes operações: a. Permitir a personalização eletrônica através de parâmetro identificador interno (label);
9. Permitir a exportação de certificados digitais armazenados no módulo criptográfico;
10. Permitir a importação de certificados digitais para a área de armazenamento do dispositivo;
11. Permitir a visualização de certificados digitais armazenados no dispositivo;
12. Permitir ao usuário, caso seja necessário, apagar chaves criptográficas e outros dados contidos no módulo criptográfico, segundo os procedimentos adequados de autenticação;
13. Permitir a troca do PIN por meio de confirmação e verificação, tanto do PIN atual, como por meio de duas inserções do novo PIN escolhido;
14. Permitir a reinicialização do papel de acesso “usuário” e conseqüentemente o valor do PIN e chaves criptográficas, mediante inserção correta do PUK;
15. Permitir a reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de novas senhas de acesso PIN e PUK.
16. Não permitir que a chave privada, se gerada no dispositivo, seja exportada, condicionando as transações que utilizam a chave privada a ocorrer dentro deste.
17. O Provedor de Serviços deve aplicar no momento da definição dos códigos PIN (Personal Identification Number) e PUK (PIN Unlock Key), os seguintes controles de qualidade: tamanho mínimo de 4 (quatro) caracteres, sensibilidade a letras maiúsculas e minúsculas do alfabeto português (Case Sensitive) e permitir o uso de caracteres especiais.
18. Quando aplicável, ou seja, quando vier inicializado com PIN e/ou PUK padrão, o módulo criptográfico deve forçar que, no primeiro acesso, o proprietário altere o PIN e/ou PUK padrão.
19. Por questões de segurança (contra-ataques de adivinhação do PIN por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PIN do papel de acesso usuário após, no máximo, 5 tentativas malsucedidas.
20. Suportar os navegadores Microsoft Internet Explorer (versão 9.0 e superiores), Mozilla (versão 24 e superiores), Chrome (versão 34 e superiores) e Safari para versão do sistema operacional Mac OS X v10.5 e superiores.

Certificado Digital tipo A1

Com a evolução dos sistemas em meio digital tornou-se preponderante implementar uma forma de garantir a integridade, confiabilidade e autenticidade das informações em meios tecnológicos;

A tecnologia atual, capaz de prover tais características, é a certificação digital, um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também validade jurídica de documentos e informações em meios eletrônicos;

O certificado digital funciona como identidade virtual, permitindo a identificação segura e inequívoca do usuário, de uma mensagem ou transação em meio eletrônico. No tocante ao certificado de equipamento garante com a mesma segurança a identificação de servidores Web (SSL) e Aplicações;

No Brasil, foi estabelecido pela Medida Provisória nº 2.202-2, de 24 de agosto de 2001, a ICP-Brasil, gerida pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil), que atua na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil, inclusive nos aspectos de normalização e nos procedimentos administrativos, técnicos, jurídicos e de segurança, que forma a cadeia de confiança da ICP-Brasil;

A tecnologia do “webservice” possibilita a integração entre diferentes sistemas, proporcionando a interação máquina-máquina através da rede de computadores. Esta tecnologia permitiu que sistemas desenvolvidos em linguagens e plataformas diferentes realizem a troca de dados no mesmo formato.

6 - REQUISITOS LEGAIS

1. Lei Federal nº 8.666/1993: institui normas gerais para licitações e contratos na Administração Pública e dá outras providências;
2. Lei Federal nº 10.520/2002: institui a modalidade de licitação denominada pregão eletrônico para aquisição de bens e serviços comuns e dá outras providências;
3. Lei Federal nº 12.846/2013: dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;
4. Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
5. Decreto nº 3.996, de 31 de outubro de 2001 - Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal; e
6. 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;
7. Decreto nº 7.579/2011: dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP, do Poder Executivo federal;
8. Decreto 7.746/2012: regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios e práticas para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;
9. Decreto nº 8.420/2015: regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências;
10. Decreto nº 9.507/2018: dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;
11. Decreto nº 9.739/2019: estabelece medidas de eficiência organizacional para o aprimoramento da administração pública federal direta, autárquica e fundacional, estabelece normas sobre concursos públicos e dispõe sobre o Sistema de Organização e Inovação Institucional do Governo Federal – SIORG;
12. Instrução Normativa SLTI/MP nº 05, de 27 de junho de 2014: dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral e suas alterações;
13. Instrução Normativa SEGES/MP nº 05, de 26 de maio de 2017: dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

14. Instrução Normativa SEGES/ME nº 01, de 10 de janeiro de 2019: dispõe sobre Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações;
15. Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019: dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal; e
16. Instrução Normativa SGD/ME nº 02, de 4 de abril de 2019: Regulamenta o art. 9º-A do Decreto nº 7.579, de 11 de outubro de 2011, e o art. 22, § 10 do Decreto nº 7.892, de 23 de janeiro de 2013, e dispõe sobre a composição e as competências do Colegiado Interno de Referencial Técnico; e
17. Instrução Normativa nº 6, de 11 de agosto de 2017 do Instituto Nacional de Tecnologia da Informação – ITI que dispôs sobre a validação de solicitação de certificados para servidores públicos da ativa e militar da união.

7 - ANÁLISE COMPARATIVA DE SOLUÇÕES (CENÁRIOS POSSÍVEIS)

A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-01/2019/SGD, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

ALTERNATIVA A: Realização de licitação para contratação de serviços de certificação digital

Tanto os certificados digitais para pessoa física (com mídia, sem mídia e em nuvem) tem a comercialização autorizada pelo ITI para diversas empresas privadas no mercado, de modo que o serviço pode ser contratado inclusive através da modalidade de licitação do tipo pregão eletrônico.

Entretanto a emissão de certificado para pessoa física com armazenamento em nuvem e emissão através do Sistema SIGEPE ainda não são ofertados por empresas privadas que, no momento, ofertam essa modalidade de certificação mediante os processos convencionais de validação de identidade.

Embora isso, por ser uma alternativa considerada viável, a realização de licitação para contratação de serviços de certificação digital será objeto da análise comparativa de custos adiante.

ALTERNATIVA B: Contratação direta do Serpro para prestação de serviços de certificação digital

O SERPRO é uma empresa pública criada com o fim específico de prover serviços de tecnologia da informação e comunicação, conforme disposto no art. 1º da Lei nº 5.615/1970:

Art. 1º O serviço Federal de Processamento de Dados (SERPRO), criado pela Lei nº 4.516, de 1 de dezembro de 1964, empresa pública, vinculada ao Ministério da Fazenda, tem por objeto a execução de serviços de tratamento de informações e processamento de dados, através de computação eletrônica ou eletromecânica, a prestação de assistência no campo de sua especialidade.

Dentre os diversos serviços de Tecnologia da Informação e Comunicação prestados pelo SERPRO estão aqueles que envolvem o provimento das certificações digitais pretendidas neste Estudo Técnico. Ademais, a Lei nº 8.666/1993 possibilita a dispensa de licitação para contratação do Serpro:

Art. 24. É dispensável a licitação:

[...]

VIII - para a aquisição, por pessoa jurídica de direito público interno, de bens produzidos ou serviços prestados por órgão ou entidade que integre a Administração Pública e que tenha sido criado para esse fim específico em data anterior à vigência desta Lei, desde que o preço contratado seja compatível com o praticado no mercado;

Por conseguinte, por ser uma alternativa considerada viável, a contratação direta do Serviço Federal de Processamento de Dados – Serpro para provimento de serviços de certificação digital será objeto da análise comparativa de custos adiante.

Um importante diferencial negocial dos certificados e-CPF emitidos pelo SERPRO é a Autoridade de Registro (AR) integrada ao Sistema SIGEPE, que permite a realização dos processos de validação de identidade, autorização de emissão e emissão do certificado seja feita diretamente através do SIGEPE sem a necessidade de atuação de um Agente de Registro ou deslocamento físico do usuário para procedimento de validação presencial.

8 - ANÁLISE COMPARATIVA DE CUSTOS

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-01/2019/SGD, e inclui:

1. comparação de custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção; e
2. memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

| ALTERNATIVA | BEM/SERVIÇO | TCO |
|-------------|--|----------------------|
| A | Realizar licitação para contratação do serviço de certificação digital | R\$ 14.066,76 |
| B | Contratar o SERPRO | R\$ 6.544,00 |

Memória de cálculo

Alternativa A: Realizar licitação para contratação do serviço de certificação digital

| ITEM | BEM/SERVIÇO | UNIDADE | R\$ UNITÁRIO MÉDIO | FONTE 1 | R\$ UNITÁRIO (FONTE 1) | FONTE 2 | R\$ UNITÁRIO (FONTE 2) | FONTE 3 | R\$ UNITÁRIO (FONTE 3) |
|------|---|---------|---------------------|-----------------------------------|------------------------|---|------------------------|--|------------------------|
| 1 | Certificados digitais e-CPF A3, com validade de 36 meses, com fornecimento de mídia do tipo Token, padrão ICP-Brasil. | UN | R\$ 144,19 | Pregão 32/2020 FUND. OSWALDO CRUZ | R\$ 290,57 | Pregão nº 5/2020, UASG 158157 - IFRJ | R\$ 70,00 | Pregão nº 79/2020, UASG 150182 - PRÓ-REITORIA DE ADMINISTRAÇÃO | R\$ 72,00 |
| 2 | Certificação Digital e-CPF A3, com validade de 36 meses, armazenado em nuvem, padrão ICP-Brasil. | UN | R\$ 195,61 | Pregão 32/2020 FUND. OSWALDO CRUZ | R\$ 105,00 | Pregão nº 5/2020, item 3, UASG 158134 - IFS | R\$ 282,00 | Pregão nº 14/2019, UASG 925869 - TJ-RN | R\$ 199,83 |
| 3 | Certificação Digital para equipamento, tipo A1, com vigência de 12 meses (Padrão ICP-Brasil) | UN | R\$ 1.402,46 | Pregão 43/2020 TJDF | R\$ 2.019,00 | Pregão nº 659/2019, UASG 238014 - DATAPREV | R\$ 1.070,40 | Pregão 39/2020, UASG 925007 - TJMT | R\$ 1.118,00 |

Alternativa B: Contratar o SERPRO

| ITEM | BEM/SERVIÇO | UNIDADE | R\$ UNITÁRIO |
|------|---|---------|--------------|
| 1 | Certificados digitais e-CPF A3, com validade de 36 meses, com fornecimento de mídia do tipo Token, padrão ICP-Brasil. | UN | R\$ 256,00 |
| 2 | e-CPF A3- Nuvem, Validade: 3 anos | UN | R\$ 179,90 |
| 3 | Certificação Digital para equipamento, tipo A1, com vigência de 12 meses (Padrão ICP-Brasil) | UN | R\$ 1.254,00 |

Além dos certificados A3 convencionais, o SERPRO fornece certificados integrados ao SIGEPE. É uma modalidade especial de emissão de certificados digitais para servidores públicos federais.

A modalidade de aquisição é mais fácil, rápida e totalmente online, sem a necessidade de presença física para comprovação de identidade. Segue tabela comparativa de preços:

| ITEM | BEM/SERVIÇO | UNIDADE | MODELO CONVENCIONAL R\$ UNITÁRIO | MODELO SIGEPE R\$ UNITÁRIO |
|------|---|---------|-------------------------------------|-------------------------------|
| 1 | Certificados digitais e-CPF A3, com validade de 36 meses, com fornecimento de mídia do tipo Token | UN | R\$ 256,00 | R\$ 67,00 |
| 2 | NeID - PF e PJ - A3 - 3 anos sem AR - Mercado Público | UN | R\$ 179,90 | R\$ 79,00 |
| 3 | Certificação Digital para equipamento, tipo A1, com vigência de 12 meses (Padrão ICP-Brasil) | UN | R\$ 1.254,00 | N/A |

9 - DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

Como estratégia de fornecimento, após analisar as alternativas disponíveis e seus respectivos custos, a Equipe de Planejamento da Contratação RECOMENDA que o serviço seja obtido mediante contratação direta do Serviço Federal de Processamento de Dados – SERPRO, por meio de aceite do CONTRATO DE ADESÃO ao respectivo serviço.

Justificativa da escolha

Para consolidar sua atuação como um provedor de serviços de Tecnologia da Informação e Comunicação, a CGTI tem como desafios fundamentais oferecer amplo acesso a serviços sob demanda, ao mesmo tempo em que deve zelar pela melhoria contínua da qualidade dos serviços e controlar os custos desses serviços. Nesse cenário, o gerenciamento de certificação digital é um dos importantes serviços administrados pela CGTI, cujo atual processo de provimento necessita ser aprimorado.

A certificação em nuvem é uma tecnologia moderna, que vem sendo orientada pelo Ministério da Economia, como mecanismo de autenticação para Sítios públicos. Com exceção do certificado A3 em nuvem, vários fornecedores públicos ou privados poderiam ofertar a solução que é única e padronizada pela ICP-Brasil, porém, visando a redução de custos e complexidade com a etapa de registro pretendida por esse órgão, o SERPRO atualmente é o único fornecedor capaz de entregar essa solução com integração ao SIGEPE, inviabilizando uma competição ou comparação com outros fornecedores.

Tal integração possibilitou ao SERPRO obter significativa vantagem competitiva em relação às demais Autoridades Certificadoras, uma vez que a integração ao SIGEPE elimina o custo de remuneração dos Agentes de Certificação e possibilitando redução do custo do serviço e, conseqüentemente, redução do seu preço de comercialização.

Além de tudo, de acordo com o estudo realizado em 2015 pelo Instituto de Negócios Públicos, o custo médio do processo licitatório é de R\$ 14.351,50 (quatorze mil, trezentos e cinquenta e um reais e cinquenta centavos).

Vantajosidade econômica

Ao compararmos os preços propostos pelo SERPRO em relação aos preços obtidos em pesquisa de mercado, chegamos à conclusão de que, em valores globais, é estimada uma economia de 54% em relação aos menores preços praticados do mercado.

Não incidência nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 1/2019

Cabe também registrar, neste documento, que o objeto da pretendida contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 1/2019, transcritos abaixo:

"Art. 3º Não poderão ser objeto de contratação:

I - mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12; e

II - o disposto no art. 3º do Decreto nº 9.507, de 2018, inclusive gestão de processos de TIC e gestão de segurança da informação.

Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.

Art. 4º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da solução de TIC seja objeto de contratação, a contratada que provê a solução de TIC não poderá ser a mesma que avalia, mensura ou apoia a fiscalização."

Cumprimento às diretrizes específicas de planejamento da contratação da IN SGD/ME nº 1/2019

A Instrução Normativa nº 01/2019/SGD/ME trouxe recomendações obrigatórias quanto às contratações de envolvem licenciamento de software e serviços agregados (Item 1 do Anexo da IN SGD/ME nº 01/2019), solução de autenticação para serviços públicos digitais (item 2 do Anexo da IN SGD/ME nº 01/2019), serviços de desenvolvimento, sustentação e manutenção de software (item 3 do Anexo da IN SGD/ME nº 01/2019) e infraestrutura de centro de dados, serviços em nuvem, sala cofre ou sala segura (item 4 do Anexo da IN SGD/ME nº 01/2019), as quais têm peso vinculatório conforme definido no §2º do art. 8º da norma:

§ 2º As contratações de soluções de TIC devem atender às normas específicas dispostas no Anexo e observar os guias, manuais e modelos publicados pelo Órgão Central do SISP.

Portanto, o escopo desse ESTUDO TÉCNICO contemplará as recomendações contidas no citado Anexo, bem como *guias, manuais e modelos publicados pelo Órgão Central do SISP.*

10 - BENEFÍCIOS ESPERADOS

Benefícios a serem alcançados

Com a contratação da solução através da estratégia sugerida são esperados os seguintes benefícios:

1. Redução dos custos de emissão de certificado digital, devido ao modelo operacional utilizado;
2. Redução dos procedimentos para emissão de certificados digitais, devido ao modelo de autoridade certificadora integrada ao SIGEPE;
3. Fornecimento de alternativa de certificação que propicia maior mobilidade aos usuários de certificado digital (certificado armazenado em nuvem);

11 - RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS/SERVIÇOS CONTRATADOS:

| ITEM | BEM/SERVIÇO | UNIDADE | QTD |
|------|---|---------------------|-----|
| 1 | Certificados digitais e-CPF A3, AR integrada ao RH , com validade de 36 meses, com fornecimento de mídia, padrão ICP-Brasil. | Certificado emitido | 20 |
| 2 | NeoID - PF e PJ - A3 - 3 anos sem AR - Mercado Público | Certificado emitido | 50 |
| 3 | Certificado Digital para equipamento, tipo A1, com vigência de 12 meses (Padrão ICP-Brasil) | Certificado emitido | 1 |

Os certificados digitais A3 (NEOID, E-CPF com Token e E-CPF sem Token) serão fornecidos sob demanda, e o quantitativo por item será utilizado conforme a efetiva necessidade do contratante.

A estimativa de certificados emitidos teve como base a quantidade de usuários que atualmente utilizam os sistemas estruturantes do governo federal e precisam executar tarefas com o uso de certificado digital, conforme tabela abaixo:

- 20 perfis na SOA;
- 10 para Ministro e Gabinete
- 10 para Secretário Executivo e gabinete;
- 10 para reserva técnica;
- 1 para servidor de aplicação do MCOM

Sugere-se manter 20 certificados A3 com token para atender demandas específicas que venham a surgir. Destaca-se que o pagamento é sob demanda.

12 - ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO

| ITEM | BEM/SERVIÇO | UNIDADE | QTD ANUAL | R\$ UNITÁRIO | R\$ TOTAL |
|--------------|---|---------|-----------|--------------|---------------------|
| 1 | Certificados digitais e-CPF A3, AR integrada ao RH , com validade de 36 meses, com fornecimento de mídia, padrão ICP-Brasil. | UN | 20 | R\$ 67,00 | R\$ 1.340,00 |
| 2 | NeoID - PF e PJ - A3 - 3 anos sem AR - Mercado Público | UN | 50 | R\$ 79,00 | R\$ 3.950,00 |
| 3 | Certificado Digital para equipamento, tipo A1, com vigência de 12 meses (Padrão ICP-Brasil) | UN | 1 | R\$ 1.254,00 | R\$ 1.254,00 |
| TOTAL | | | | | R\$ 6.544,00 |

Assinaturas

Assinam o presente documento os integrantes técnico e requisitante da Equipe de Planejamento da Contratação, conforme Art. 11, parágrafo 2º da IN SGD nº 1/2019.

Integrante Técnico

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD nº 1/2019, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

ÉDER GILLIAN SILVA BESERRA

(Assinatura eletrônica registrada na Seção de Assinaturas)

Integrante Requisitante

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD nº 1/2019 e atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade. Os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

LUIZ FERNANDO BASTOS COURA

(Assinatura eletrônica registrada na Seção de Assinaturas)

AUTORIDADE MÁXIMA DA ÁREA DE TIC

A Subsecretária de Planejamento e Tecnologia da Informação certifica a plena observância do prescrito no Art. 11 da IN SGD 01/2019 na elaboração do documento em tela.

O presente planejamento está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área responsável priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a aquisição proposta.

WANESSA QUEIROZ DE SOUZA OLIVEIRA

(Assinatura eletrônica registrada na Seção de Assinaturas)



Documento assinado eletronicamente por **Luiz Fernando Bastos Coura, Coordenador de Governança de Tecnologia da Informação**, em 29/01/2021, às 20:45 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Eder Gillian Silva Beserra, Coordenador de Infraestrutura e Segurança**, em 29/01/2021, às 20:45 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira, Subsecretária de Planejamento e Tecnologia da Informação**, em 01/02/2021, às 14:04 (horário oficial de Brasília), com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site <http://sei.mctic.gov.br/verifica.html>, informando o código verificador **6448415** e o código CRC **009FF16B**.

AVISO

Para ser considerado válido, este Estudo Técnico Preliminar da Contratação deverá conter as assinaturas eletrônicas dos integrantes técnico e requisitante indicados para compor a Equipe de Planejamento da Contratação e pela autoridade máxima da área de TIC, nos termos da Instrução Normativa nº 01, de 04 de abril de 2019.