Anexo I do Edital

TERMO DE REFERÊNCIA

Processo Administrativo nº 23090.021643/2020-82

Contratação de Certificados Digitais e-CPF e e-CNPJ

Lavras, setembro de 2020

Histórico de Revisões

Data	Versão	Descrição	Autor
22/09/2020	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação

Sumário

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 1/2019

1 – OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa especializada na prestação de serviços de emissão de certificados digitais. Esses serviços são: a renovação e emissão de certificados digitais do tipo A3, e-CPF, padrão ICP-Brasil, com validade de 36 meses e sem fornecimento do Token Criptográfico; e a emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ, padrão ICP-Brasil, com fornecimento de Token criptográfico, com validade de 36 meses.

2 – DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1 Bens e serviços que compõem a solução

Id.	Descrição do Bem ou Serviço	Código CATSER	Quantidade	Métrica ou Unidade
1	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento para renovação, com validade por 3 anos.	27219	20	Unidade
2	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de token criptográfico USB para armazenamento do certificado, com validade por 3 anos.	27189	79	Unidade
3	Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de token criptográfico USB para armazenamento do certificado, com validade por 3 anos.	27197	2	Unidade

2.1.1. A utilização da certificação digital é fundamental para que os servidores da Universidade Federal de Lavras (UFLA) acessem os diversos sistemas da Administração

Pública Federal (SCDP, SIAPE, SIAFI, Receita Federal e Comprasnet), que permitem o funcionamento das atividades institucionais.

2.1.2. A solução será adquirida na forma de contratação de serviço e contemplará a emissão de certificados do nível A3, e-CPF (com e sem fornecimento de dispositivo físico de armazenamento do tipo USB) e e-CNPJ (com fornecimento de dispositivo físico de armazenamento do tipo USB), com validade de 3 anos, em conformidade com o padrão ICP-Brasil.

3 – JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. O Certificado digital é uma assinatura eletrônica que utiliza chaves criptográficas para confirmar a identidade de uma pessoa física (e-CPF) ou pessoa jurídica (e-CNPJ). O certificado digital pode ser armazenado em um dispositivo do tipo Token. Os Tokens e certificados digitais são utilizados por servidores da UFLA para reforçar a segurança da informação e garantir um acesso mais seguro a diversos sistemas estruturantes da administração pública federal, tais como: Sistema de Concessão de Diárias e Passagens (SCDP); Sistema Integrado de Administração de Pessoal (SIAPE); Sistema de Gestão de Pessoas (SIGEPE), Sistema Integrado de Administração Financeira (SIAFI), Portal de Compras - COMPRASNET, Receita Federal, entre outros.

3.1.2. Até o ano de 2017, os certificados digitais utilizados pela UFLA eram emitidos pelo SERPRO e custeados pelo Ministério do Planejamento, Desenvolvimento e Gestão do governo federal. No entanto, conforme Ofício Circular nº 468/2016-MP, a emissão de certificado digital não será mais custeada pelo referido Ministério. Desde então, cada órgão deve realizar a respectiva previsão orçamentária para a emissão dos certificados digitais e realizar o planejamento da contratação conforme preconiza a IN 01/2019 da SGD/ME .

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica. Objetivo da Estratégia de Governo Digital 2020 - 2022 (Revogou a Política de Governança Digital, instituída pelo Decreto nº 8.638, de 15 de janeiro de 2016).

Objetivo 15.4	Aprimorar a Segurança da Informação e Comunicação, por meio da governança dos riscos de TIC. Objetivo estratégico do Plano de Desenvolvimento Institucional (PDI) 2016 - 2020 da UFLA (Planejamento Estratégico Institucional).

ALINHAMENTO AO PDTIC 2017 - 2020			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A.90.101	6) Criação das Normas de Uso dos Recursos Criptográficos em Segurança da Informação e Comunicações	M.101	Criar e revisar as normas de Segurança da Informação da UFLA
A.97.134	1) Planejamento da contratação 2) Licitação	M.134	Contratar serviços de emissão de certificados digitais do tipo A3, eCPF e eCNPJ, padrão ICP-Brasil, com e sem fornecimento de dispositivo físico de armazenamento.

ALINHAMENTO AO PAC 2020 e 2021	
Item	**Descrição**
4246	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA (PAC 2020)
10	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA (PAC 2021)
4530	EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA (PAC 2020)
11	EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA (PAC 2021)
4531	EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURIDICA (PAC 2020)

3.2.1. Entende-se que o objeto em questão não se trata de oferta digital de serviços públicos, sendo assim, não é necessário integração à Plataforma de Cidadania Digital, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016.

3.3. Estimativa da demanda

3.3.1. Foi realizado o levantamento da demanda de certificado digital, com e sem dispositivo de armazenamento, com os servidores docentes e técnico-administrativos da UFLA, do dia 29 de julho de 2020 ao dia 10 de agosto de 2020, por meio de questionário eletrônico. O levantamento de demanda foi divulgado por meio de e-mail institucional e também no sítio eletrônico da UFLA. Foram identificadas 20 demandas para renovação de certificados com validade até o fim de 2021.

3.3.2. O levantamento também apontou a necessidade de emissão de 79 novos certificados digitais e-CPF, com fornecimento de dispositivos físicos de armazenamento. Foi identificada também a necessidade de emissão de 2 novos certificados digitais e-CNPJ, com fornecimento de dispositivos físicos de armazenamento. Essa previsão para emissão dos certificados digitais e-CNPJ é uma estratégia de segurança para reposição, caso ocorra alguma perda ou dano com os certificados digitais e-CNPJ utilizados atualmente na instituição.

3.3.3. Uma vez que a contratação vigente se encerrará em 8 de novembro de 2020, não sendo assim possível atender toda a demanda supracitada, é fundamental proceder com a contratação de empresa especializada para a emissão de certificados digitais do tipo A3, e-CPF e e-CNPJ. A impossibilidade de acesso aos Sistemas da Administração Pública Federal por parte dos servidores que utilizam a certificação digital poderá prejudicar fortemente as atividades administrativas da Instituição.

ESTIMATIVA DE NECESSIDADE DE CERTIFICAÇÃO DIGITAL		
Item	**Descrição do Bem ou Serviço**	**Total**
1	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento para renovação, com validade por 3 anos.	20
2	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de token criptográfico USB para armazenamento do certificado, com validade por 3 anos.	79
3	Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de token criptográfico USB para armazenamento do certificado, com validade por 3 anos.	2

3.3.4. Para o Item 1 “Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento

de dispositivo físico de armazenamento para Renovação, com validade por 3 anos" ressalta-se que o dispositivo físico de armazenamento já existente na UFLA é o token. Caberá à empresa licitante ofertar o seu preço considerando apenas a emissão do certificado, sem o fornecimento da mídia criptográfica.

3.4. Parcelamento da Solução de TIC

3.4.1. A solução mostra-se técnica e economicamente viável para o parcelamento em 3 itens, independentes entre si, conforme quadro da seção 3.3. Desta forma, haverá melhor aproveitamento do mercado e ampliação da competitividade.

3.4.2. Apesar dos esforços da equipe de planejamento em levantar um quantitativo próximo à realidade, as incertezas acerca dos impactos da mudança de gestão na Universidade, em relação aos ocupantes de cargos cuja utilização de certificados digitais é fundamental para o exercício da função, os quantitativos apresentados são meras estimativas. Por isso, não se constituem, em hipótese alguma, compromissos futuros para a UFLA, razão pela qual não poderão ser exigidos, nem considerados como valor para pagamento mínimo, podendo sofrer alterações de acordo com as necessidades da Contratante, sem que isso justifique qualquer indenização à Contratada.

3.4.3. Diante do supracitado, optou-se que a licitação ocorra por meio de Registro de Preços. O Decreto nº 7.892, de 23 de janeiro de 2013, traz a seguinte redação em seu Art. 3º:

"O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;

II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;

III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração."

3.4.4. Entende-se, portanto, que a contratação em questão se insere nos incisos I, II e IV do referido Decreto.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. Acesso aos sistemas da Administração Pública Federal – Os sistemas estruturantes da Administração Pública Federal exigem o certificado digital dos servidores que possuem função de gestor. Sem o certificado digital não é possível ter o acesso de gestor.

3.5.2. Aumentar a segurança da informação e comunicação – A geração da chave de criptografia, do certificado digital do tipo A3, oferece mais segurança para acessar os sistemas de

informação. No certificado digital A3, a geração da chave é feita em um hardware separado, o que faz com que haja mais proteção dos dados.

4 – ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Os certificados serão utilizados pelos servidores da UFLA e permitirão o acesso destes aos diversos sistemas da Administração Pública Federal, que exigem a certificação digital para determinados perfis (Sistema de Concessão de Diárias e Passagens - SCDP, Sistema de Integrado de Administração de Pessoal – SIAPE, Sistema Integrado de Administração Financeira - SIAFI, Receita Federal, Portal de Compras – Comprasnet, Receita Federal), garantindo os princípios de segurança da informação (autenticidade, confidencialidade e integridade) dos atos públicos da Administração.

4.1.2. O acesso a tais sistemas é essencial para possibilitar a continuidade de atividades fundamentais para a Instituição.

4.2. Requisitos de Capacitação

4.2.1. A Contratada deverá ter capacidade técnica para orientar o titular do certificado digital, durante a validação presencial de documentos do servidor, sobre as melhores práticas de utilização, visando evitar o mau uso do certificado e do respectivo dispositivo de armazenamento.

4.3. Requisitos Legais

4.3.1. A certificação digital oferece as seguintes garantias: autenticidade do emissor e do receptor da transação ou do documento, integridade dos dados contidos na transação ou no documento e confidencialidade entre as partes. Ela é fundamental para que os servidores da Universidade Federal de Lavras (UFLA) que possuem perfis que necessitam deste tipo de autenticação acessem os diversos sistemas da Administração Pública Federal (SCDP, SIAPE, SIAFI, Receita Federal e Comprasnet), nos quais ocorrem transações que permitem o funcionamento das atividades institucionais. Portanto, a solução tem de estar em conformidade com as seguintes políticas, modelos e padrões de governo: infraestrutura de Chaves Públicas Brasileira e ICP-Brasil.

4.4. Requisitos de Manutenção

Não se aplica.

4.5. Requisitos Temporais

4.5.1. A Contratada deverá realizar a validação presencial para emissão dos certificados em, no máximo, 7 (sete) dias úteis após o contato para agendamento pelo servidor da UFLA.

4.5.2. Após a validação presencial do certificado, a Contratada terá, no máximo, 2 (dois) dias úteis para entregar o certificado ao servidor da UFLA.

4.6. Requisitos de Segurança

4.6.1. A solução deverá ser aderente às normas do Comitê Gestor da ICP-Brasil e estar em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017. Deverá ainda seguir as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. O software de gerenciamento do dispositivo deverá estar no idioma Português do Brasil.

4.8. Requisitos de Arquitetura Tecnológica

Requisitos Tecnológicos da Solução de TIC	
Item	**Descrição**
1. Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento para renovação, com validade por 3 anos.	1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 1.2. Nível: A3. 1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 1.5. Tipo: e-CPF. 1.6. Ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da

	República, Ministério da Fazenda, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios, entre outros. 1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal). 1.8. Os certificados digitais deverão ser compatíveis com os tokens modelo: Token StarSign USB – G&D Burti, StarSign Crypto – USB-Token S, SafeNet iKey 2032 e SafeNet Token 5100/5110, já existentes na UFLA.
2. Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de token criptográfico USB para armazenamento do certificado, com validade por 3 anos.	2.1. Certificado 2.1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de julho de 2017). 2.1.2. Nível: A3. 2.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 2.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 2.1.5. Tipo: e-CPF. 2.1.6. Ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Fazenda, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros. 2.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal). 2.2. Dispositivo Físico de armazenamento 2.2.1. Dispositivo Físico de armazenamento (token criptográfico), em modelo homologado conforme padrão ICP-Brasil e constante na lista de homologação atual disponível no site do Instituto Nacional de Tecnologia da Informação (ITI).

	2.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 2.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior. 2.2.4. Ser aderente às normas do Comitê Gestor da ICP-Brasil. 2.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2. 2.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes. 2.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas. 2.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3). 2.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas. 2.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por derivação, a partir de um código de acesso escolhido pelo titular do repositório. 2.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits. 2.2.12. Possuir carcaça resistente à água e à violação. 2.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores). 2.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores). 2.2.15. Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da Microsoft (Windows 2000 e versões superiores). 2.2.16. Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente. 2.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, de tal forma que aplicações em Java possam utilizar qualquer das

	funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE. 2.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4. 2.2.18. Possuir indicador luminoso de estado do dispositivo. 2.2.19. Assinar dados digitalmente em até 10 (dez) segundos. 2.2.20. O token criptográfico deverá possuir certificação do INMETRO. 2.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura. 2.3. Funcionalidades 2.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores. 2.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label). 2.3.3. Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres. 2.3.4. Permitir criação de senhas com caracteres alfanuméricos. 2.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos. 2.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459. 2.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo. 2.3.8. Permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key). 2.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). 2.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. 2.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores).

	2.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo. 2.3.13. Implementar mecanismo de autenticação tipo challenge-response. 2.3.14. Forçar a troca da senha padrão no primeiro acesso. 2.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos. 2.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida. 2.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. 2.4. Software 2.4.1. Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita: 2.4.1.1. gerenciamento do dispositivo; 2.4.1.2. exportação de certificados armazenados no dispositivo; 2.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; 2.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; 2.4.1.5. visualização de certificados armazenados no dispositivo; 2.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; 2.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso. 2.4.2. Deverá ser disponibilizado portal para download de drivers/softwares de forma ilimitada e gratuita. 2.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.
3. Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de token criptográfico USB	3.1. Certificado 3.1.1. Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP Brasil (em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 6 de

para armazenamento do Certificado, com validade por 3 anos.	julho de 2017). 3.1.2. Nível: A3. 3.1.3. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 3.1.4. Todos os certificados deverão ser emitidos sob a hierarquia V2. 3.1.5. Tipo: e-CNPJ. 3.1.6. Ser homologado e utilizado nos serviços eletrônicos da Receita Federal e dos principais Órgãos da Administração Pública Federal no processo de certificação digital brasileira, como Presidência da República, Ministério da Fazenda, da Economia, do Planejamento e da Defesa, Procuradoria Geral da Fazenda Nacional, Banco Central do Brasil, Justiça Federal, SERPRO, Correios entre outros. 3.1.7. Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal). 3.2. Dispositivo Físico de Armazenamento 3.2.1. Dispositivo Físico de armazenamento (Token criptográfico), em modelo homologado conforme padrão ICPBrasil e constante na lista de homologação atual disponível no site do Instituto Nacional de Tecnologia da Informação (ITI). 3.2.2. Validade: 3 (três) anos, contados a partir da data de emissão do certificado. 3.2.3. Possuir conector USB (Universal Serial Bus) tipo A, versão 1.0 (compatível com 2.0) ou superior. 3.2.4. Ser aderente às normas do Comitê Gestor da ICPBrasil. 3.2.5. Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2. 3.2.6. Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes. 3.2.7. Utilizar algoritmo simétrico 3-DES ou AES, com chaves de, no mínimo, 128 bits para cifrar as chaves privadas armazenadas. 3.2.8. Utilizar algoritmo simétrico 3DES com três chaves distintas (k1, k2 e k3). 3.2.9. Utilizar algoritmo RSA/SHA-2 ou RSA/SHA-1 para geração de assinaturas. 3.2.10. Possuir o algoritmo simétrico AES, sua chave gerada por

	derivação, a partir de um código de acesso escolhido pelo titular do repositório. 3.2.11. Ter suporte à tecnologia de chaves pública/privada (PKI), com geração on-board do par de chaves RSA de, no mínimo, 1024 bits. 3.2.12. Possuir carcaça resistente à água e à violação. 3.2.13. Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores). 3.2.14. Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores). 3.2.15. Possuir CSP - Cryptographic Services Provider para Windows (Windows 2000 e versões superiores) e em conformidade com o padrão da CryptoAPI 2.0, da Microsoft (Windows 2000 e versões superiores). 3.2.16. Possuir biblioteca de objetos compartilhados em ambiente Linux (.so) e dynamic-link library (.dll) em ambiente Windows que implemente, em sua completude, o padrão PKCS#11 v2.0 ou mais recente. 3.2.16.1. Disponibilizar driver para que os frameworks Java JCA e Java JCE se comuniquem em perfeita harmonia com a biblioteca PKCS#11 nativa do token criptográfico, de tal forma que aplicações em Java possam utilizar qualquer das funcionalidades existentes no padrão PKCS#11 por meio dos frameworks Java JCA e Java JCE. 3.2.17. Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4. 3.2.18. Possuir indicador luminoso de estado do dispositivo. 3.2.19. Assinar dados digitalmente em até 10 (dez) segundos. 3.2.20. O token criptográfico deverá possuir certificação do INMETRO. 3.2.21. Permitir conexão direta na porta USB (Universal Serial Bus), sem necessidade de interface intermediária para leitura. 3.3. Funcionalidades 3.3.1. Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores. 3.3.2. Permitir personalização eletrônica através de parâmetro identificador interno (label). 3.3.3. Permitir criação de senha de acesso ao dispositivo de, no

	mínimo, 6 (seis) caracteres. 3.3.4. Permitir criação de senhas com caracteres alfanuméricos. 3.3.5. Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos; 3.3.6. Permitir gravação de chaves privadas e certificados digitais que utilizam a versão 3 do padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 2459. 3.3.7. Armazenar chaves privadas em repositório de dados próprio, controlado pela solução, apenas certificados pertencentes a um único titular podem ser associados às chaves contidas num determinado dispositivo, sendo que no caso de certificados emitidos para pessoas jurídicas, o titular é a pessoa física responsável pela empresa. 3.3.8. Permitir inicialização e reinicialização do token criptográfico mediante a utilização de PUK (Pin Unlock Key). 3.3.9. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores). 3.3.10. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome. 3.3.11. Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores) 3.3.12. Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo. 3.3.13. Implementar mecanismo de autenticação tipo challenge-response; 3.3.14. Forçar a troca da senha padrão no primeiro acesso; 3.3.15. Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos; 3.3.16. Avisar o titular do dispositivo, a cada vez que uma função for ativada, utilizando a sua chave privada. Nesse caso, deverá haver autenticação para liberar a utilização pretendida; 3.3.17. Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do token criptográfico. 3.4. Software 3.4.1. Características do software de gerenciamento do dispositivo,

	no idioma Português do Brasil, que permita: 3.4.1.1. gerenciamento do dispositivo; 3.4.1.2. exportação de certificados armazenados no dispositivo; 3.4.1.3. importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315; 3.4.1.4. importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo; 3.4.1.5. visualização de certificados armazenados no dispositivo; 3.4.1.6. apagamento de chaves e outros dados contidos no dispositivo, após autenticação do titular; 3.4.1.7. reutilização de dispositivos bloqueados, através de apagamento total dos dados armazenados e geração de nova senha de acesso. 3.4.2. Deverá ser disponibilizado portal para download de drivers/Softwares de forma ilimitada e gratuita. 3.4.3. Garantia de 3 (três) anos, contada a partir da emissão do certificado.

4.9. Requisitos de Projeto e de Implementação

Não se aplica.

4.10. Requisitos de Implantação

4.10.1. Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores) e Linux (kernel 2.4, 2.6 e superiores).

4.10.2. Suportar, no mínimo, os seguintes navegadores: Microsoft Internet Explorer (versão 7 e superiores), Mozilla (versão 3 e superiores) e Chrome.

4.10.3. Deverá ser disponibilizado portal para download de drivers/softwares de forma ilimitada e gratuita.

4.11. Requisitos de Garantia

4.11.1. Será exigida a garantia de 3 (três) anos do certificado digital e do dispositivo físico de armazenamento, contada a partir da data do aceite definitivo dos produtos. Para o item 1 da contratação, a garantia será exigida apenas para o certificado digital emitido, uma vez que a Contratada não disponibilizará o dispositivo físico de armazenamento.

4.11.2. Em caso de necessidade de acionar a garantia, a Contratante informará à Contratada via e-mail. A Contratada terá um prazo de até 7 (sete) dias úteis, após a data da comunicação feita pela Contratante, para analisar o problema apresentado e emitir um novo certificado, se necessário.

4.11.2.1. Se houver necessidade, também deverá disponibilizar um novo dispositivo físico de armazenamento.

4.11.2.2. Se na análise do problema apresentado a Contratada constatar o mau uso, deverá apresentar provas à Contratante para que seja desobrigada de fornecer um novo certificado e/ou dispositivo de armazenamento.

4.11.2.3. Se houver bloqueio do certificado por esquecimento de senha por parte do titular ou se for apagado pelo titular, a Contratada estará desobrigada de custear as despesas do novo certificado.

4.12. Requisitos de Experiência Profissional

Não se aplica.

4.13. Requisitos de Formação da Equipe

Não se aplica.

4.14. Requisitos de Metodologia de Trabalho

4.14.1. O serviço de certificação presencial e validação de documentos de cada certificado deverá ser prestado no município de Lavras. Para fins da presente contratação, o local em que a Contratada prestará o serviço será aqui denominado “Posto de Atendimento”.

4.14.2. A Contratante não disponibilizará estrutura física, recursos materiais ou humanos para a execução do serviço.

4.14.3. A Contratada deverá disponibilizar um canal de comunicação (telefone, e-mail ou sistema de abertura de chamados) para cadastramento prévio e agendamento, em que seja suficiente um único comparecimento do servidor da UFLA ao posto de atendimento para que o certificado seja emitido.

4.14.4. A Contratante e a Contratada poderão estabelecer cronograma para a execução do objeto, desde que observadas as condições de prazos estabelecidas neste Termo de Referência.

4.15. Requisitos de Segurança da Informação

4.15.1. A solução deverá ser aderente às normas do Comitê Gestor da ICP-Brasil e estar em conformidade com a Resolução nº 123 do Comitê Gestor de Infraestrutura de Chaves Públicas

Brasileira - ICP Brasil, de 6 de julho de 2017. Também deverá seguir as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

4.16. Outros Requisitos Aplicáveis

Não se aplica.

5 – RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos.

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico.

5.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável.

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável.

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato.

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

5.2.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante.

5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária.

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

5.2.8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

5.2.9. Comunicar à Contratante, por meio da Diretoria de Tecnologia da Informação e Comunicação, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

5.2.10. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade, no que couber. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos, preferencialmente nas dependências da UFLA. Caso os produtos apresentem qualquer defeito durante o período em garantia, quaisquer ônus com materiais, peças ou componentes substituídos, supervisão técnica e/ou operacional, transporte, diárias e demais despesas decorrentes da prestação do serviço correrão por conta da Contratada. Caso necessário, a Contratada se responsabilizará pelo envio e acompanhamento dos produtos junto aos respectivos fabricantes, sendo que, quaisquer ônus com transporte, diárias e demais despesas decorrentes da prestação do serviço correrão por conta da Contratada.

5.2.11. Assinar o Termo de Sigilo e Confidencialidade e o Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes. Os referidos Termos deverão ser enviados pela Contratada no momento do envio da Ata de Registro de Preço devidamente assinados. Se, ao longo da vigência da Ata, houver outros funcionários da Contratada que venham a participar da execução dos serviços e que não tenham assinado o Termo de Ciência, a Contratada deverá enviar para a Contratante o referido documento atualizado com as

assinaturas destes funcionários.

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

5.3.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços.

5.3.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados.

5.3.3. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3. 1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível;

5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.

5.3.4. Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela contratada;

5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

5.3.5. Assinar a Ata de Registro de Preços no prazo de até 5 (cinco) dias, contados a partir da data de sua convocação, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Contratante poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de 5 (cinco) dias, a contar da data de seu recebimento.

5.3.5.1. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pela CONTRATADA, durante o seu transcurso, e desde que devidamente aceito.

6 – MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. Forma de execução e acompanhamento dos serviços

6.1.1.1. A execução dos serviços será iniciada após a assinatura da Ata de Registro de Preços e de acordo com a demanda da UFLA, mediante acionamento por Ordem de Serviço (OS) pela Contratante.

6.1.1.2. A Contratante comunicará à Contratada, via e-mail a ser designado para esse fim, identificação de servidores autorizados a realizar a gestão dos certificados digitais. Essa forma de comunicação poderá ser substituída, caso a Contratada possua sistema próprio de abertura de chamados que permita à UFLA enviar os nomes de tais servidores.

6.1.1.3. A Contratada deverá disponibilizar um canal de comunicação (telefone, e-mail ou sistema de abertura de chamados) para cadastramento prévio e agendamento, em que seja suficiente um único comparecimento do servidor da UFLA ao posto de atendimento para que o certificado seja emitido. Para casos em que for necessário mais de um comparecimento do servidor, devido a problemas alheios à vontade da Contratada, ela deverá apresentar justificativa à Contratante.

6.1.1.4. A Contratada enviará à Contratante um número único de identificação da abertura do chamado (referente ao cadastramento prévio solicitado pelo servidor da UFLA) e a Ordem de Serviço correspondente.

6.1.1.5. A Contratada deverá disponibilizar, via telefone, e-mail ou sistema de abertura de chamados, uma data e um horário para a validação presencial em seu posto de atendimento.

6.1.1.6. No momento do cadastramento, a Contratada deverá fornecer ao servidor da UFLA uma lista com todos os documentos necessários para a emissão do certificado, a fim de evitar a necessidade de mais de um comparecimento do servidor ao posto de atendimento para a conclusão do serviço.

6.1.1.7. A Contratada deverá orientar o titular do certificado, durante a validação presencial, sobre as melhores práticas de uso, evitando, assim, o mau uso de certificados digitais com seus respectivos dispositivos de armazenamento e suas consequências.

6.1.1.8. A quantidade de certificados a serem emitidos por agendamento será de apenas 01 (um) por atendimento, a critério da demanda da UFLA.

6.1.1.9. Os dispositivos de armazenamento (tokens criptográficos) deverão ser novos, de primeiro uso e em perfeitas condições de utilização, de forma a permitir completa segurança por parte da Contratante, sob pena do não recebimento definitivo dos mesmos.

6.1.1.10. A Contratada deverá disponibilizar meio para que a Contratante possa solicitar, quando necessário, um relatório com todos os números de identificação da abertura de chamados realizados, data e horário agendados para a validação dos documentos, data de realização da validação dos documentos e data de entrega do certificado, para fins de acompanhamento e fiscalização.

6.1.2. Prazos

6.1.2.1. A Contratada deverá realizar a validação presencial para emissão dos certificados em, no máximo, 7 (sete) dias úteis após o contato para agendamento pelo servidor da UFLA. Comunicar eventual impossibilidade de cumprimento deste prazo, o qual somente será justificável quando decorrer de caso fortuito ou de força maior, conforme disposições contidas no Código Civil Brasileiro ou por fatos de responsabilidade da UFLA. Encaminhar, na ocorrência dos fatos acima, o pedido de prorrogação do prazo, de forma escrita e em até 05 (cinco) dias corridos antes de findar aquele originalmente exigido e, em ambos os casos, com justificativas.

6.1.2.2. Após a validação presencial de documentos do servidor, a Contratada terá, no máximo, 2 (dois) dias úteis para entregar o certificado ao servidor da UFLA. Comunicar eventual impossibilidade de cumprimento do prazo, o qual somente será justificável quando decorrer de caso fortuito ou de força maior, conforme disposições contidas no Código Civil Brasileiro ou por fatos de responsabilidade da UFLA. Encaminhar, na ocorrência dos fatos acima, o pedido de prorrogação do prazo de entrega, de forma escrita e em até 01 (um) dia corrido antes de findar aquele originalmente exigido e, em ambos os casos, com justificativas.

6.1.2.3. Até o quinto dia útil de cada mês, a Contratada enviará à Contratante, em forma digital, lista com os nomes dos servidores da UFLA que receberam certificados digitais no mês anterior, especificando:

a) A Ordem de Serviço e o tipo de serviço prestado:

I. emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento - renovação, com validade por 3 anos;

II. emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de Token criptográfico para armazenamento do certificado, com validade por 3 anos;

III. emissão de certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de Token criptográfico para armazenamento do certificado, com validade por 3 anos;

b) Data em que o serviço foi prestado.

6.1.2.4. Em caso de necessidade de acionamento da garantia, a Contratante informará à Contratada via e-mail, para abertura de Ordem de Serviço (OS). A Contratada terá um prazo de 7 (sete) dias úteis, após a data da comunicação feita pela Contratante, para emitir um novo

certificado e um novo dispositivo físico de armazenamento, caso seja necessário. Se na análise do problema apresentado a Contratada constatar o mau uso, deverá apresentar provas à Contratante para que seja desobrigada de fornecer um novo certificado e/ou dispositivo de armazenamento. Se houver bloqueio do certificado por esquecimento de senha por parte do titular ou se for apagado pelo titular, a Contratada estará desobrigada de custear as despesas do novo certificado. Em caso de eventual impossibilidade de cumprimento do prazo, o qual somente será justificável quando decorrer de caso fortuito ou de força maior, conforme disposições contidas no Código Civil Brasileiro ou por fatos de responsabilidade da UFLA, a Contratante deverá encaminhar o pedido de prorrogação do prazo de entrega, de forma escrita e em até 05 (cinco) dias corridos antes de findar aquele originalmente exigido e, em ambos os casos, com justificativas.

6.1.3. Horários

6.1.3.1. A Contratada deverá disponibilizar posto de atendimento para validação presencial de documentos e emissão do certificado, cujo horário de funcionamento seja, ao menos, das 8 (oito) às 17 (dezessete) horas, de segunda à sexta-feira, exceto feriados. No caso do cadastramento prévio a ser solicitado pelo servidor da UFLA, que será realizado por telefone, e-mail ou sistema de abertura de chamados, os horários a serem disponibilizados pela empresa também deverão ser, pelo menos, os supracitados.

6.1.4. Locais da Prestação do Serviço

6.1.4.1. O serviço de certificação presencial e validação de documentos de cada certificado deverão ser prestados no município de Lavras. Considerando que o serviço de certificação digital é essencial para o funcionamento das atividades da Instituição, é fundamental que ele esteja disponível sempre que houver demanda por parte da Contratante, observados os prazos e horários descritos nos itens 6.1.1, 6.1.2 e 6.1.3.

6.1.4.2. Ressalta-se que a Contratante não disponibilizará estrutura física, recursos materiais ou humanos para a execução do serviço, dentro ou fora das dependências da Contratante, sendo tais de responsabilidade exclusiva da Contratada.

6.1.4.3. Em hipótese alguma os servidores da Contratante se deslocarão para outra cidade para obter o serviço. Tal exigência visa à economicidade para a Administração, evitando custos com diárias e despesas com locomoção para os servidores se deslocarem a outras cidades para realizar a validação presencial dos documentos, bem como o comprometimento da carga horária de trabalho, custeada pelo contribuinte, ainda que a empresa custeie as referidas despesas.

6.1.5. Documentação mínima exigida

6.1.5.1. A Contratada deverá ser credenciada na ICP-Brasil.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1. O detalhamento acerca da estimativa da demanda encontra-se no tópico 3.3 deste documento. Conforme justificado no referido documento, os quantitativos apresentados são meras estimativas e serão licitados por Sistema de Registro de Preços. Por isso, não se constituem, em hipótese alguma, compromissos futuros para a UFLA, razão pela qual não poderão ser exigidos, nem considerados como valor para pagamento mínimo, podendo sofrer alterações de acordo com as necessidades da Contratante, sem que isso justifique qualquer indenização à Contratada.

6.3. Mecanismos formais de comunicação

6.3.1. As comunicações entre a Contratante e a Contratada ocorrerão, preferencialmente, via e-mail. No entanto, a Contratada também deverá disponibilizar central telefônica para contato, cujo horário de funcionamento seja, ao menos, das 8 (oito) às 17 (dezessete) horas, de segunda à sexta-feira, exceto feriados. Serão adotadas Ordens de Serviços.

6.4. Manutenção de Sigilo e Normas de Segurança

6.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

O **Termo de Compromisso**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS II e III.

7 – MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. Os serviços serão recebidos provisoriamente pelo requisitante, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.1.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as

especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de até 10 (dez) dias úteis, a contar da notificação do licitante vencedor, às suas custas, sem prejuízo da aplicação das penalidades.

7.1.3. Caso a substituição não ocorra no prazo definido no item anterior, estará o licitante vencedor incorrendo em atraso na entrega, sujeito à aplicação das sanções previstas neste Termo de Referência.

7.1.4. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, após a verificação e consequente aceitação mediante termo circunstanciado.

7.1.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7.2. Procedimentos de Teste e Inspeção

7.2.1. Os procedimentos de teste, verificação e inspeção serão realizados conforme descrição estabelecida no Item 4 deste Termo de Referência.

7.3. Níveis Mínimos de Serviço Exigidos

Indicador 1 – IAV – Indicador de Atraso para a Validação presencial de documentos e emissão de certificado digital	
Tópico	**Descrição**
Finalidade	Garantir que a validação de documentos do servidor da UFLA ocorra no prazo previsto neste Termo de Referência, uma vez que o acesso aos sistemas do governo federal é fundamental para manter atividades essenciais da Instituição.
Meta a cumprir	Até 7 (sete) dias úteis, após o agendamento.
Instrumento de medição	Ordem de Serviço emitida pela Contratante.
Forma de acompanhamento	Comunicação à DGTI/UFLA, formalizada por servidor que tenha verificado o descumprimento do prazo e relatório emitido pela Contratada, conforme disposto no item 6.1.1.10 deste Termo de Referência.
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.

Mecanismo de Cálculo (métrica)	**IAV = $\frac{\text{TEVD – TEST}}{\text{TEST}}$** Onde: **IAV** – Indicador de Atraso da Validação presencial de documentos e emissão do certificado digital; **TEVD** – Tempo para Validação de Documentos – corresponde ao período utilizado pela Contratada para executar a validação dos documentos, contabilizado da data do agendamento feito pelo servidor da Contratante até a data de realização da validação dos documentos; **TEST** – Tempo Estimado para a validação presencial dos documentos, conforme estipulado no Termo de Referência. O cálculo será por dia útil de atraso.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante. Obs4: A Contratada deverá comunicar eventual impossibilidade de cumprimento do prazo, conforme exposto no item 6.1.2.1 deste Termo de Referência.
Início de Vigência	A partir da data do agendamento com emissão da OS.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAV**: De 0 a 0,10 – Pagamento integral; De 0,11 a 0,20 – Glosa de 2,5% sobre o valor da Ordem de Serviço - OS; De 0,21 a 0,30 – Glosa de 05% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 7,5% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 10% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 15% sobre o valor da OS.

Indicador 2 – IAE – Indicador de Atraso de Entrega de certificado digital	
Tópico	**Descrição**
Finalidade	Garantir que o certificado seja entregue ao servidor da UFLA no prazo previsto neste Termo de Referência, uma vez que o acesso aos sistemas do governo federal é fundamental para manter atividades essenciais da Instituição.
Meta a cumprir	Até 2 (dois) dias úteis, após a validação presencial de documentos.
Instrumento de medição	Ordem de Serviço emitida pela Contratante.
Forma de acompanhamento	Comunicação à DGTI/UFLA, formalizada por servidor que tenha verificado o descumprimento do prazo e relatório emitido pela Contratada, conforme disposto no item 6.1.1.10 deste Termo de Referência.
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.

Mecanismo de Cálculo (métrica)	**IAE = TEX – TEST / TEST** Onde: **IAE** – Indicador de Atraso de Entrega do certificado digital; **TEX** – Tempo de Entrega – corresponde ao prazo utilizado pela Contratada para entregar o certificado digital ao titular, contabilizado da data após a validação presencial dos documentos até a data de entrega do certificado; **TEST** – Tempo Estimado para a entrega do certificado, conforme estipulado no Termo de Referência. O cálculo será por dia útil de atraso.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante. Obs4: A Contratada deverá comunicar eventual impossibilidade de cumprimento do prazo, conforme exposto no item 6.1.2.2 deste Termo de Referência.
Início de Vigência	A partir da data em que ocorrer a validação presencial de documentos do servidor da UFLA.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAE**: De 0 a 0,10 – Pagamento integral; De 0,11 a 0,20 – Glosa de 2,5% sobre o valor da Ordem de Serviço - OS; De 0,21 a 0,30 – Glosa de 05% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 7,5% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 10% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 15% sobre o valor da OS.

Indicador 3 – IAT – Indicador de Atraso de Troca de produto	
Tópico	**Descrição**
Finalidade	Garantir que a troca seja efetuada no prazo estipulado neste Termo de Referência, evitando que o servidor da UFLA fique sem acesso aos sistemas do Governo Federal.
Meta a cumprir	Até 7 (sete) dias úteis, após a data da comunicação feita pela Contratante, observando o disposto no item 6.1.2.4 deste Termo de Referência.
Instrumento de medição	Ordem de Serviço emitida pela Contratante.
Forma de acompanhamento	Comunicação à DGTI/UFLA, formalizada por servidor que tenha verificado o descumprimento do prazo e relatório emitido pela Contratada, conforme disposto no item 6.1.1.10 deste Termo de Referência.
Periodicidade	Mensalmente.

Mecanismo de Cálculo (métrica)	**IAT = TTP – TEST / TEST** Onde: **IAT** – Indicador de Atraso de Troca do produto; **TTP** – Tempo para a Troca do produto – corresponde ao período utilizado pela Contratada para realizar a troca do produto, da data de notificação pela Contratante (e-mail) até a data de disponibilização do novo produto - nova emissão de certificado e/ou novo dispositivo físico de armazenamento; **TEST** – Tempo Estimado para a troca do produto, conforme estipulado no Termo de Referência. O cálculo será por dia útil de atraso.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: A Contratada deverá comunicar eventual impossibilidade de cumprimento do prazo, conforme exposto no item 6.1.2.4 deste Termo de Referência.
Início de Vigência	A partir da data de envio do e-mail por parte da Contratante, solicitando o acionamento da garantia.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador **IAT**: De 0 a 0,10 – Pagamento integral; De 0,11 a 0,20 – Glosa de 1% sobre o valor da Fatura Mensal; De 0,21 a 0,30 – Glosa de 2,5% sobre o valor da Fatura Mensal; De 0,31 a 0,50 – Glosa de 5% sobre o valor da Fatura Mensal; De 0,51 a 1,00 – Glosa de 7% sobre o valor da Fatura Mensal; Acima de 1 – Será aplicada Glosa de 10% sobre o valor da Fatura Mensal.

7.4. Sanções Administrativas

7.4.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

7.4.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.4.1.2. ensejar o retardamento da execução do objeto;

7.4.1.3. falhar ou fraudar na execução da ata;

7.4.1.4. comportar-se de modo inidôneo;

7.4.1.5. cometer fraude fiscal.

7.4.2. Pela inexecução total ou parcial do objeto da Ata de Registro de Preços, a Administração pode aplicar à Contratada as seguintes sanções:

7.4.2.1. advertência por escrito, quando do não cumprimento de quaisquer das obrigações consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

7.4.2.2. multa de:

7.4.2.2.1. 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

7.4.2.2.2. 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;

7.4.2.2.3. 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

7.4.2.2.4. 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

7.4.2.2.5. as penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si;

7.4.2.3. suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

7.4.2.4. sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

7.4.2.4.1. a sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.4.1 deste Termo de Referência;

7.4.2.5. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

7.4.3. As sanções previstas nos subitens 7.4.2.1, 7.4.2.3, 7.4.2.4 e 7.4.2.5 poderão ser aplicadas à Contratada juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.4.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

7.4.4.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

7.4.4.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

7.4.4.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

7.4.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

7.4.6. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

7.4.6.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

7.4.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.4.9. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

7.4.10. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.
7.4.11. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.
7.4.12. As penalidades serão obrigatoriamente registradas no SICAF.

7.5. Do Pagamento

7.5.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.5.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

7.5.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.5.3.1. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

7.5.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.5.6. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.5.7. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

7.5.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá

realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.9. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.5.10. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

7.5.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

7.5.11.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

7.5.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.5.12.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

7.5.13. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) I = $\frac{(6 / 100)}{365}$ I = 0,00016438

TX = Percentual da taxa anual
= 6%

7.6. Procedimentos para Retenção ou Glosa no Pagamento

7.6.1. As glosas porventura aplicadas, conforme previstas no item 7.3 deste Termo de Referência, serão descontadas dos pagamentos devidos pela UFLA ou cobradas diretamente da Contratada penalizada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas.

7.6.2. Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados e a aceitação da justificativa ficará a critério da UFLA, que examinará a legalidade da conduta da Contratada.

7.6.3. Comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela UFLA, conforme procedimento esboçado no subitem anterior, a Contratada ficará isenta das glosas mencionadas.

8 – ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. As pesquisas de preços foram obtidas no Painel de Preços e em mídias especializadas. As formas para obtenção das estimativas de preços, dados das pesquisas de preços, detalhamento dos cálculos, bem como as justificativas encontram-se pormenorizadas no item 5 do Estudo Técnico Preliminar, Anexo IV do Edital.

Id.	Descrição do Bem ou Serviço	Quantidade	Unidade de Medida	Valor Unitário Estimado	Valor Total Estimado
1	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, sem fornecimento de dispositivo físico de armazenamento para Renovação, com validade por 3 anos.	20	Unidade	R$ 142,00	R$ 2.840,00

2	Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de token criptográfico USB para armazenamento do Certificado, com validade por 3 anos.	79	Unidade	R$ 330,55	R$ 26.113,45
3	Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de token criptográfico USB para armazenamento do Certificado, com validade por 3 anos.	2	Unidade	R$ 325,00	R$ 650,00
Custo total estimado				**R$ 29.603,45**	

9 – ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. Não se aplica por se tratar de uma compra utilizando o Sistema de Registro de Preços. A dotação orçamentária será informada no momento da contratação.

10 – DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS E DO CONTRATO

10.1. A ata registro de preços terá vigência de 1 (um) ano, contado a partir de sua assinatura.

10.2. Os contratos decorrentes da ata de registro de preços terão prazo de vigência de 1 (um) ano, contado a partir de sua assinatura, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

11 – DO REAJUSTE DE PREÇOS

11.1. Os valores decorrentes da ata de registro de preços e do contrato são fixos e irreajustáveis.

12 – DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1.Regime, Tipo e Modalidade da Licitação

12.1.1. Será utilizada a modalidade Pregão, na forma Eletrônica, pelo Sistema de Registro de Preços, onde os objetos a serem adquiridos enquadram-se na classificação de bens comuns, nos termos do parágrafo único do art. 1 da Lei nº 10.520/2002 e do inciso II, do art. 3 do Decreto nº 10.024/2019.

12.1.2. A licitação será dividida em itens, conforme tabela e condições apresentadas no presente Termo de Referência, facultando-se ao licitante a participação em quantos itens forem de seu interesse.

12.1.3. O objeto da licitação será adjudicado por item, mediante critério de menor preço.

12.1.4. Não será permitida adesão à presente licitação.

12.2 Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.2.1. Decreto nº 7.174/2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal: aplicável. Em seu artigo 5º, o supracitado Decreto traz a seguinte redação:

> "Art. 5º. Será assegurada preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 1991, para fornecedores de bens e serviços, observada a seguinte ordem:
>
> I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;
>
> II - bens e serviços com tecnologia desenvolvida no País; e
>
> III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.
>
> Parágrafo único. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos do caput terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso."

12.2.2. Isto posto, em relação ao Decreto 7.174/2010, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8°.

12.2.3. Lei Complementar nº 123/2006 - Institui o Estatuto Nacional da Microempresa e da

Empresa de Pequeno Porte: aplicável. A referida Lei, traz em seu artigo 48:

> "Art. 48. Para o cumprimento do disposto no art. 47 desta Lei Complementar, a administração pública:
>
> I - deverá realizar processo licitatório destinado exclusivamente à participação de microempresas e empresas de pequeno porte nos itens de contratação cujo valor seja de até R$ 80.000,00 (oitenta mil reais);
>
> (...)
>
> III - deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte."

12.2.4. Assim, em respeito à norma, os itens 1, 2 e 3 serão destinados exclusivamente à disputa por microempresas (ME) e empresas de pequeno porte (EPP).

12.3 Critérios de Qualificação Técnica para a Habilitação

	Critério	Justificativa
12.3.1.	Comprovação perante o Instituto Nacional de Tecnologia da Informação (ITI) ou pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) que ateste a licitante é credenciada, sendo autorizada a emitir certificados digitais e que faz parte da estrutura da ICP-Brasil. Caso se entenda necessário, o pregoeiro verificará a veracidade das informações no sítio eletrônico https://estrutura.iti.gov.br/ ou sítio eletrônico oficial do ITI ou ICP-Brasil. Não serão aceitas empresas em fase de credenciamento.	Conformidade com a norma complementar 09/IN01/DSIC/GSI/PR. Garantir o atendimento aos requisitos técnicos dos certificados especificados neste Termo de Referência.

13 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria/PROPLAG nº 242, de 13 de julho de 2020, retificada pela Portaria/PROPLAG nº 243, de 14 de julho de 2020, reconduzida pela Portaria/PROPLAG nº 299, de 03 de setembro de 2020.

13.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

_____ **Integrante Requisitante** Plínio Márcio Braga Torres **Matrícula/SIAPE: 1629350**	_____ **Integrante Técnico** Fernando Elias de Oliveira **Matrícula/SIAPE: 2076633**	_____ **Integrante Administrativo** Cassia Marques Batista Nobre **Matrícula/SIAPE: 1675322**

Autoridade Máxima da Área de TIC
_____ Erasmo Evangelista de Oliveira **Matrícula/SIAPE: 1307332**

Aprovo,

Autoridade Competente
_____ Márcio Machado Ladeira **Matrícula/SIAPE: 1127313**