

COLETA

DE

ESTIMATIVAS

Coleta de Estimativas: **2026/2448** Tipo: **Registro de Preços** Situação: **Liberada** Data: **07/10/2026**

Coordenado por: **SMATI - SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO, TECNOLOGIA E INOVAÇÃO**

Especificação: **Fornecimento e garantia de certificados digitais ICP-Brasil e tokens.**

Itens Coletados			SMATI	Estimados		
Nº	Un.	Produto		Qtde Total	Unit. (R$)	Total (R$)
1	UN	68685 - CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A1	50	50	57,66	2.883,00
2	UN	68684 - CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A1	20	20	56,02	1.120,40
3	UN	68687 - CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A3	200	200	48,33	9.666,00
4	UN	68686 - CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A3	10	10	68,80	688,00
5	UN	68691 - TOKEN USB PARA CERTIFICADO DIGITAL	50	50	46,48	2.324,00
Total Estimado (R$):			16.681,40	16.681,40		

Coleta : 2026/2448 **Situação** : Encerrada

Data : 07/10/2026

Especificaçã : Fornecimento e garantia de certificados digitais ICP-Brasil e tokens.

Item	Produto	Unidade	Quantidade
1	68685 - CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A1: a) Certificado digital do tipo A1 para pessoa física (e-CPF). b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros. d) Deve ser gerado e armazenado em arquivo digital, permitindo sua instalação e utilização em ambiente computacional compatível, bem como a exportação do certificado e de sua chave privada, quando permitido pelas políticas e procedimentos aplicáveis. e) Deve ter validade de 1 (um) ano, contada a partir da emissão do certificado. f) O presente item engloba o serviço de autoridade de certificação e registro. g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada. g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais. g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.	UN	50,00
2	68684 - CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A1: a) Certificado digital do tipo A1 para pessoa jurídica (e-CNPJ). b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros. d) Deve ser gerado e armazenado em arquivo digital, permitindo sua instalação e utilização em ambiente computacional compatível, bem como a exportação do certificado e de sua chave privada, quando permitido pelas políticas e procedimentos aplicáveis. e) Deve ter validade de 1 (um) ano, contada a partir da emissão do certificado. f) O presente item engloba o serviço de autoridade de certificação e registro. g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada. g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais. g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.	UN	20,00

3	68687 - CERTIFICADO DIGITAL PARA PESSOA FÍSICA DO TIPO A3: a) Certificado digital do tipo A3 para pessoa física (e-CPF). b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros. d) Deve ser compatível com a emissão e utilização em dispositivo criptográfico compatível com os requisitos e certificações aplicáveis da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI), quando utilizado em token criptográfico. e) Deve ter validade de 2 (dois) anos ou o prazo máximo disponível conforme cadeia de certificados vigente, contada a partir da emissão do certificado. f) O presente item engloba o serviço de autoridade de certificação e registro. g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada. g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais. g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.	UN	200,00
4	68686 - CERTIFICADO DIGITAL PARA PESSOA JURÍDICA DO TIPO A3: a) Certificado digital do tipo A3 para pessoa jurídica (e-CNPJ). b) Deve ser emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). c) Deve permitir a utilização para assinatura de documentos eletrônicos, e-mails e acesso a sistemas que utilizem certificados digitais para autenticação, incluindo sistemas governamentais como Receita Federal do Brasil, Caixa Econômica Federal, Banco do Brasil, entre outros. d) Deve ser compatível com a emissão e utilização em dispositivo criptográfico compatível com os requisitos e certificações aplicáveis da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI), quando utilizado em token criptográfico. e) Deve ter validade de 2 (dois) anos ou o prazo máximo disponível conforme cadeia de certificados vigente, contada a partir da emissão do certificado. f) O presente item engloba o serviço de autoridade de certificação e registro. g) A emissão/renovação do certificado digital, poderá ser realizada de forma presencial, eletrônica ou por videoconferência, com apoio da equipe técnica da contratada. g.1) Caso a emissão seja realizada de forma eletrônica ou por videoconferência, devem ser proporcionados os recursos tecnológicos necessários para sua realização. Caso o equipamento do usuário não suporte a execução de tais recursos, a atividade deve ser realizada de forma presencial, sem cobrança de custos adicionais. g.2) A atividade deve ocorrer na sede das secretarias onde os servidores exercem suas atividades.	UN	10,00

5	68691 - TOKEN USB PARA CERTIFICADO DIGITAL: a) Dispositivo criptográfico com interface USB, compatível com portas USB-A existentes nos equipamentos utilizados pelo Município. b) Deve ser capaz de gerar e utilizar, de forma segura, chaves criptográficas, bem como armazenar e utilizar certificados digitais A3 (e-CPF, e-CNPJ e/ou e-PJ), emitidos por autoridade certificadora credenciada pela ICP-Brasil. c) Dispor de drivers e software utilitário de gerenciamento do dispositivo compatíveis com os sistemas operacionais Windows 11 64 bits, macOS e Linux Ubuntu 64 bits, nas versões oficialmente suportadas pelo fabricante durante a vigência contratual, em idioma português brasileiro. d) O software utilitário de gerenciamento deve dispor de funcionalidades que permitam consultar informações gerais do token e, conforme suportado pelo dispositivo, realizar operações de inicialização, gerenciamento dos certificados, alteração do PIN e do PUK, desbloqueio do PIN mediante PUK e demais operações de gerenciamento previstas pelo fabricante. e) Deve ser compatível com os navegadores Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera e Safari, em suas versões estáveis, permitindo acesso a sistemas que requeiram autenticação por meio de certificado digital. f) Deve ser compatível com aplicações de assinatura digital de documentos PDF que utilizem certificados digitais e padrões criptográficos compatíveis com ICP-Brasil, incluindo o Adobe Acrobat Reader quando disponível para o sistema operacional utilizado. g) A instalação do driver e do software utilitário de gerenciamento do dispositivo não deve interferir com outros dispositivos que, porventura, já estejam instalados no sistema operacional, e não deverá exigir a desativação de mecanismos de segurança do sistema operacional, como antivírus, firewall ou mecanismos de proteção equivalentes, nem exigir privilégios administrativos permanentes para sua utilização normal. h) Deve dispor de manuais de instalação do driver e de instalação e operação do software utilitário de gerenciamento do dispositivo, com documentação específica aplicável a cada um dos sistemas operacionais referidos na letra "c". i) O dispositivo deve implementar mecanismo de bloqueio após quantidade configurada ou definida pelo fabricante de tentativas consecutivas de PIN inválido, de forma a impedir tentativas ilimitadas de autenticação. j) O dispositivo deve implementar mecanismo de proteção contra tentativas consecutivas de PUK inválido, conforme os requisitos de segurança e homologação aplicáveis ao dispositivo. k) Deve permitir a reinicialização segura do dispositivo para seu estado inicial, com remoção dos certificados e chaves privadas armazenados e possibilidade de configuração de novo PIN de acesso, conforme os procedimentos previstos pelo fabricante. l) Deve permitir a importação de certificados e respectivas chaves privadas, quando tecnicamente aplicável, para a área de armazenamento do dispositivo, a partir de arquivos no formato PKCS#12 (PFX/P12), conforme os padrões aplicáveis. m) Deve permitir a exportação dos certificados públicos armazenados no dispositivo, sem permitir a exportação das respectivas chaves privadas. n) Deve possuir capacidade de armazenamento de certificados digitais e respectivas chaves privadas suficiente para permitir a instalação e utilização simultânea de, no mínimo, 10 (dez) certificados digitais A3 distintos, sem comprometer o funcionamento e a segurança do dispositivo. o) Deve possuir garantia mínima de 1 (um) ano, contado a partir do recebimento pelo Município, contra defeitos de fabricação e funcionamento.	UN	50,00