CAMARA MUNICIPAL DE MACAE - RJ

Estudo Técnico Preliminar 24/2026

1. Informações Básicas

Número do processo: 510/2026

2. Descrição da necessidade

2.1. Contratação de Certificados Digitais e-CPF e e-CNPJ

O certificado digital é uma assinatura eletrônica que utiliza chaves criptográficas para confirmar a identidade de uma pessoa física (e-CPF) ou de uma pessoa jurídica (eCNPJ). O certificado digital pode ser armazenado em um dispositivo do tipo token. As demandas se concentram em: Vereadores, Diretores, Coordenadores e Presidente desta casa, para o formato e-CPF com Token; Câmara Municipal de Macaé e Fundo Especial da Câmara Municipal de Macaé para o formato e-CNPJ com Token.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Contabilidade	Nilton Sampaio Vieira

4. Descrição dos Requisitos da Contratação

4.1 Os Serviços incluem:

Autenticação por meio de certificado digital no sistema estruturante do governo: SIAPENET

- Autenticação por meio de certificado digital no sistema estruturante do governo: SIAFI.

- Autenticação por meio de certificado digital no sistema estruturante do governo: Compras.gov.br.

- Autenticação por meio de certificado digital no sistema da Receita Federal do Brasil.

- Autenticação por meio de certificado digital nos demais sistemas estruturantes do governo, além dos retrocitados.

- Gestão de chaves e senhas durante os 36 meses de validade do certificado.

4.2 - Certificado digital do tipo A3, padrão ICP-Brasil, e-CPF, com fornecimento de dispositivo físico para armazenamento do certificado, com validade por 3 anos.

4.2.1 Do Certificado:

- Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil (em conformidade com a Resolução nº 65 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, de 9 de junho de 2009).

- Nível: A3.

- Validade: 3 (três) anos, contados a partir da data de emissão do certificado.

- Todos os certificados deverão ser emitidos sob a hierarquia V2.

- Tipo: e-CPF.

- 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.

- Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal, entre outros).

PROCURADORIA GERAL
11
CÂMARA MUNICIPAL DE NATAL

PROCESSO
Nº 530/26
Fls 11
ASSINATURA

r.2.2 Do Dispositivo Físico de Armazenamento:

- Dispositivo físico de armazenamento, 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).

- Validade: 3 (três) anos, contados a partir da data de emissão do certificado.

- Ser aderente às normas do Comitê Gestor da ICP-Brasil.

- Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

- Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.

- Possuir carcaça resistente à água e à violação.

- Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).

- Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).

- 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).

- 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.

- 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.

- Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.

- Possuir indicador luminoso de estado do dispositivo.

- Assinar dados digitalmente em até 10 (dez) segundos.

- O dispositivo físico de armazenamento deverá possuir certificação do INMETRO.

4.2.3 Das Funcionalidades:

- Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.

- Permitir personalização eletrônica através de parâmetro identificador interno (label).

- Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.

- Permitir criação de senhas com caracteres alfanuméricos.

- Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.

- 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.

- 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.

- Permitir inicialização e reinicialização do dispositivo físico de armazenamento do certificado mediante a utilização de PUK (Pin Unlock Key).

- Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores), Linux (kernel 2.4, 2.6 e superiores) e Mac OS (10.0 e superiores).

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

- Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores).

- Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo.

- Implementar mecanismo de autenticação tipo challenge-response.

- Forçar a troca da senha padrão no primeiro acesso.

- Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos.

- 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.

- Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do dispositivo físico de armazenamento.

4.2.4 Do Software de Gestão:

- Por questão de segurança, todos os serviços do software de gestão serão realizados pela contratada.

- Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:

- Gerenciamento do dispositivo;

- Exportação de certificados armazenados no dispositivo;

- Importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;

- Importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;

- Visualização de certificados armazenados no dispositivo;

- Remoção de chaves e outros dados contidos no dispositivo, após autenticação do titular;

- Reutilização de dispositivos bloqueados, por meio de apagamento total dos dados armazenados e geração de nova senha de acesso.

- Garantia da prestação do serviço por 3 (três) anos, contados a partir da emissão do certificado.

4.3 - Certificado digital do tipo A3, padrão ICP-Brasil, e-CNPJ, com fornecimento de dispositivo físico para armazenamento do certificado, com validade por 3 anos.

4.3.1 Do Certificado:

- Emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP Brasil (em conformidade com a Resolução nº 65 do Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira - ICP Brasil, de 9 de junho de 2009).

- Nível: A3.

- Validade: 3 (três) anos, contados a partir da data de emissão do certificado.

- Todos os certificados deverão ser emitidos sob a hierarquia V2.

- Tipo: e-CNPJ.

- 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.

- Atender a demanda de assinatura digital em sistemas estruturantes da Administração Pública Federal (SCDP, SIAFI, Siapenet, ComprasNet, Receita Federal, entre outros).

4.3.2 Do Dispositivo Físico de Armazenamento:

- Dispositivo físico de armazenamento, 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).

- Validade: 3 (três) anos, contados a partir da data de emissão do certificado.

- Ser aderente às normas do Comitê Gestor da ICP-Brasil.

- Seguir, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

- Possuir capacidade de armazenamento de certificados e chaves privadas de, no mínimo, 32 Kbytes.

- Possuir carcaça resistente à água e à violação.

- Fornecer driver disponível para o sistema operacional Linux (kernel 2.4, 2.6 e versões superiores).

- Fornecer driver disponível para o sistema operacional Microsoft Windows (2000 e versões superiores).

- 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).

- 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.

- 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.

- Possuir compatibilidade com as especificações ISO 7816, partes 1, 2, 3 e 4.

- Possuir indicador luminoso de estado do dispositivo.

- Assinar dados digitalmente em até 10 (dez) segundos.

- O dispositivo físico de armazenamento deverá possuir certificação do INMETRO.

PROCURADORIA GERAL CÂMARA MUNICIPAL DE MACAÉ
14
PROCESSO Nº 510/26 Fls 14 ASSINATURA

4.3.3 Das Funcionalidades:

Permitir a exportação automática de certificados armazenados no dispositivo para o Certificate Store do ambiente Microsoft Windows 2000 e versões superiores.

- Permitir personalização eletrônica através de parâmetro identificador interno (label).

- Permitir criação de senha de acesso ao dispositivo de, no mínimo, 6 (seis) caracteres.

- Permitir criação de senhas com caracteres alfanuméricos.

- Permitir geração de chaves, protegidas por PINs (Personal Identification Number), compostos por caracteres alfanuméricos.

- 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.

- 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.

Permitir inicialização e reinicialização do dispositivo físico de armazenamento do certificado mediante a utilização de PUK (Pin Unlock Key).

- Ter compatibilidade com sistemas operacionais Windows (2003, XP, Vista, 7 e superiores), Linux (kernel 2.4, 2.6 e superiores) e Mac OS (10.0 e superiores).

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

- Possuir middleware para Windows 2000 e versões superiores e Linux (kernel 2.4, 2.6 e superiores).

- Possuir ativação de funções que utilizem as chaves privadas, que somente possam ser realizadas após autenticação da identidade do titular do dispositivo.

- Implementar mecanismo de autenticação tipo challenge-response.

- Forçar a troca da senha padrão no primeiro acesso.

- Bloquear o dispositivo, após 5 (cinco) tentativas de autenticação com códigos inválidos.

- 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.

- Bloquear a exportação da chave privada, condicionando as transações que forem utilizadas dentro do dispositivo físico de armazenamento.

4.3.4 Do Software de Gestão:

- Por questão de segurança, todos os serviços do software de gestão serão realizados pela contratada.

- Características do software de gerenciamento do dispositivo, no idioma Português do Brasil, que permita:

- Gerenciamento do dispositivo;

- Exportação de certificados armazenados no dispositivo;

- Importação de certificados em formato PKCS#7 para área de armazenamento do dispositivo, de acordo com a RFC 2315;

- Importação de certificados em formato PKCS#12 para área de armazenamento do dispositivo;

Visualização de certificados armazenados no dispositivo;

- Remoção de chaves e outros dados contidos no dispositivo, após autenticação do titular;

- Reutilização de dispositivos bloqueados, por meio de apagamento total dos dados armazenados e geração de nova senha de acesso.

- Garantia da prestação do serviço por 3 (três) anos, contados a partir da emissão do certificado.

4.4. Certificado digital do tipo A1, padrão ICP-Brasil, e-CNPJ, com validade por 12 meses.

4.4.1 Armazenamento: Instalado diretamente nos computadores da Câmara Municipal de Macaé.

4.4.2. Acessar o Conectividade Social (FGTS), Receita Federal, e-CAC, assinar contratos digitais e demais órgãos governamentais.

5. Levantamento de Mercado

5.1. Soluções

Solução 1 - Serviço de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF e e-CNPJ, com fornecimento de token USB como dispositivo físico de armazenamento.

A solução 1 provê a emissão de certificado digital e-CPF e e-CNPJ e o armazenamento de certificados digitais do tipo A3, e-CPF e e-CNPJ, em um token USB, dispositivo portátil em formato chaveiro, capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas as chaves, essas estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do token (seu hardware criptográfico), além de protegê-las de riscos como roubo ou violação. Para o acesso ao certificado digital, é necessária apenas a conexão do token USB a uma porta USB no periférico a ele conectado.

Solução 2 - Serviço de emissão de certificados digitais do tipo A3, padrão ICP-Brasil, e-CPF e e-CNPJ, com fornecimento de cartão como dispositivo físico de armazenamento, acompanhado de leitora de cartão.

A solução 2 provê a emissão de certificados digitais e-CPF e e-CNPJ, e o armazenamento de certificados digitais do tipo A3 em um smart card, ou seja, um hardware em formato estilo "cartão de crédito", capaz de armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas as chaves, essas estarão totalmente protegidas, pois não será possível exportálas ou retirá-las do cartão (seu hardware criptográfico), além de protegê-las de riscos como roubo ou violação. Para o acesso ao certificado digital armazenado no cartão, é necessário que a solução venha acompanhada de uma leitora de smart cards, que se trata do equipamento responsável por fazer a gravação e a leitura dos certificados digitais que ficam armazenados dentro dos smart cards. A leitora de cartões possui uma interface USB, sendo responsável por realizar a troca de dados entre o smart card e o periférico a ele conectado.

Solução 3 - Certificado em Nuvem.

Essa solução precisa de rede de internet estável, tanto para o computador, quanto para o dispositivo móvel previamente autorizado. Além disso, é necessária uma verificação de segurança de pelo menos dois níveis, isto é, por meio do uso de uma senha (PIN) utilizada pelo usuário e de uma segunda validação recebida por meio de um aplicativo em seu dispositivo móvel. Essa solução utilizaria bens privados dos usuários, isto é, dispositivos móveis e, até mesmo, dados móveis, o que inviabiliza a contratação. Outro ponto importante é que nem sempre será utilizado nas dependências da Câmara Municipal de Macaé, com isso ficando suscetível a instabilidade da rede. Por esses motivos elencados, esta comissão descartou esse cenário na análise comparativa.

PROCURADORIA GERAL 16 CÂMARA MUNICIPAL DE MACAÉ

5.2. Solução Escolhida: Solução 1

5.2.1 Justificativa da Escolha:

Os certificados digitais armazenados em cartão e em token USB realizam exatamente as mesmas operações e possuem as mesmas funcionalidades, o que muda é a praticidade no uso de cada um deles. A principal diferença entre o token USB e o cartão é que o token USB não precisa da utilização de uma leitora, já que ele se conecta diretamente à porta USB, padrão existente em qualquer computador. Já o cartão, precisa de um dispositivo leitor de cartões USB para ser utilizado.

PROCESSO Nº 510/26 Fls 16 ASSINATURA

6. Descrição da solução como um todo

6.1.

Item	Código Item	Descrição	Unidade	Quantidade
01	27197	Emissão de Certificado Digital A3, com Token Pessoa Jurídica E-CNPJ.	UN	04
02	27189	Emissão de Certificado Digital A3, com Token Pessoa Física E-CPF.	UN	30
03	27162	Emissão de Certificado Digital A1, Pessoa Jurídica E-CNPJ.	UN	08

6.2 - Serviço de certificação presencial e validação de documentos de cada certificado deverão ser prestados no município de Macaé. Para fins da presente contratação, o local em que a Contratada prestará o serviço será aqui denominado "Posto de Atendimento". 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 descritos nos requisitos 6.8 e 6.9, abaixo. Ficará facultada a contratante a realização da certificação pessoal em loco, no prédio da Câmara Municipal de Macaé. Ressalta-se que neste caso a Contratante disponibilizará apenas a estrutura física, ficando a cargo exclusivo da contratada os recursos materiais ou humanos para a execução do serviço. 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.

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

6.4 - 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 Câmara Municipal de Macaé 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.

6.5 - 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 ou em loco na Câmara Municipal de Macaé.

6.6 - A Contratada deverá disponibilizar posto de atendimento para validação presencial 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 Câmara Municipal de Macaé, 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.

6.7 - No momento do cadastramento, a Contratada deverá fornecer ao servidor da Câmara Municipal de Macaé uma lista com todos os documentos necessários para a emissão do certificado, a fim de evitar a necessidade de retorno do servidor ao posto de atendimento para a conclusão do serviço.

6.8 - 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.

6.9 - 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 Câmara Municipal de Macaé.

6.10 - Após a validação presencial do certificado, a Contratada terá, no máximo, 2 (dois) dias úteis para entregar o certificado ao servidor da Câmara Municipal de Macaé.

6.11 - Até o quinto dia útil de cada mês, a Contratada deverá enviar à Contratante, em forma digital, lista com os nomes dos servidores da Câmara Municipal de Macaé que receberam certificados digitais no mês anterior, especificando:

a) o tipo de serviço prestado, isto é: emissão de certificado digital, e-CPF, com fornecimento de dispositivo físico de armazenamento; emissão de certificados digital, e-CNPJ, com fornecimento de dispositivo físico de armazenamento.

b) data em que o serviço foi prestado.

PROCURADORIA GERAL CÂMARA MUNICIPAL DE MACAÉ 18 / 3.

PROCESSO Nº 510/26 Fls 18

6.12 - A quantidade de certificados a serem emitidos por agendamento será de apenas 01 (um) por atendimento, a critério da demanda da Câmara Municipal de Macaé, podendo haver mais de um agendamento no mesmo dia.

6.13 - Os dispositivos de armazenamento 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.

7. Estimativa das Quantidades a serem Contratadas

7.1. O quantitativo foi encaminhado pelo setor requisitante via DFD 016/2026. Informamos que esta Equipe não possui membro com a expertise técnica necessária para avaliar os quantitativos solicitados.

7.2.

Item	Código Item	Descrição	Unidade	Quantidade
01	27197	Emissão de Certificado Digital A3, com Token Pessoa Jurídica E-CNPJ.	UN	04
02	27189	Emissão de Certificado Digital A3, com Token Pessoa Física E-CPF.	UN	30
03	27162	Emissão de Certificado Digital A1, Pessoa Jurídica E-CNPJ.	UN	08

8. Estimativa do Valor da Contratação

Valor (R$): 10.100,00

8.1. Os valores foram retirados do DFD 016/2026. Devendo ser aferido com maior precisão pelo setor de cotação desta casa no decorrer do processo.

8.2.

Item	Código Item	Descrição	Unid	Quantidade	Valor Unit	Valor Total
01	27197	Emissão de Certificado Digital A3, com Token Pessoa Jurídica E-CNPJ.	UN	04	R$ 250,00	**R$ 1.000,00**
02	27189	Emissão de Certificado Digital A3, com Token Pessoa Física E-CPF.	UN	30	R$ 250,00	**R$ 7.500,00**
03	27162	Emissão de Certificado Digital A1, Pessoa Jurídica E-CNPJ.	UN	08	R$ 200,00	**R$ 1.600,00**
					Valor Total Anual	**R$ 10.100,00**

9. Justificativa para o Parcelamento ou não da Solução

9.1. Em regra, conforme inciso II do art. 47 da Lei n 14.133, de 2021, do parcelamento, quando for tecnicamente viável e economicamente vantajoso.

9.2. O disposto não se aplica a presente demanda por se tratar de serviço que requer padronização e atendimento personalizado.

PROCURADORIA GERAL CÂMARA MUNICIPAL DE MACAÉ 19 2.

PROCESSO Nº 530/26 Fls 19 ASSINATURA

10. Contratações Correlatas e/ou Interdependentes

10.1. Não há contratações correlatas tendo em vista se tratar de serviço independente, incluindo todos os insumos e equipamentos necessários.

11. Alinhamento entre a Contratação e o Planejamento

11.1. Os presentes serviços constam no plano anual de contratações PCA 930552-39/2026, sob os IDs 473, 474 e 475. Inserido através do DFD 016/2026.

12. Benefícios a serem alcançados com a contratação

12.1. Desde o início da informatização dos processos nesta casa Legislativa, mostrou-se necessário adquirir certificados digitais para que os usuários do processo eletrônico da Câmara Municipal de Macaé possam assinar os documentos eletrônicos e acessar determinados sistemas. Tais certificados para usuários precisam ser gerados e armazenados em tokens para atendimento das normas da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), criada pela Medida Provisória n°2.200-2, de 24 de agosto de 2001. Outro fator importante é a elevação da 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.

13. Providências a serem Adotadas

13.1. Considerando se tratar de um serviço independente, não há necessidade de nenhuma providência prévia.

14. Possíveis Impactos Ambientais

14.1. Trata-se o presente de serviço eletrônico, onde não há impacto ambiental direto. O serviço eletrônico elimina a necessidade do uso de papel, colaborando assim para a preservação do meio ambiente.

PROCURADORIA GERAL
20
CÂMARA MUNICIPAL DE MACAÉ

PROCESSO
Nº 510/26
Fls 20
ASSINATURA

15. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

15.1. Justificativa da Viabilidade

Concluímos este estudo com posicionamento favorável a contratação nos moldes já utilizados por esta casa. Apesar de termos identificado algumas possibilidades de alteração na tecnologia, após análise, nenhuma apresentou vantajosidade, sendo assim, seguimos conforme a contratação remanescente.

16. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Despacho: Portaria 004/2026 da Câmara Municipal de Macaé

JULIANO FARIAS PEREIRA GASPIO

Presidente da Equipe de Planejamento

Assinou eletronicamente em 30/04/2026 às 11:06:26.

Despacho: Portaria 004/2026 da Câmara Municipal de Macaé

FABIOLA DE OLIVEIRA LIMA

Membra da Equipe de Planejamento

Assinou eletronicamente em 30/04/2026 às 11:08:32.

Despacho: Portaria 004/2026 da Câmara Municipal de Macaé

PROCESSO
Nº 510/26
Fls 21
ASSINATURA

FERNANDO TADEU PINHEIRO VIEIRA

Membro da Equipe de Planejamento

Assinou eletronicamente em 04/05/2026 às 11:39:00.

Despacho: Portaria 004/2026 da Câmara Municipal de Macaé

PROCURADORIA GERAL
21
CÂMARA MUNICIPAL DE MACAÉ

ALEXANDRE MACHADO FERREIRA

Membro da Equipe de Planejamento

Assinou eletronicamente em 30/04/2026 às 11:08:59.

Despacho: Portaria 004/2026 da Câmara Municipal de Macaé

CRISTIANE DE OLIVEIRA CAVOUR

Membra da Equipe de Planejamento

Assinou eletronicamente em 30/04/2026 às 11:21:50.

NILTON SAMPAIO VIEIRA

Diretor de Contabilidade