

ESP-DIR TEC INFORMAÇÃO E COMUNICAÇÃO - DTIC

Estudo Técnico Preliminar 37/2025**1. Informações Básicas**

Número do processo: 017.00126365/2025-03

2. Plano de Contratações Anual

O objeto da contratação está previsto no Plano de Contratações Anual 2026, nos termos do Decreto estadual nº67.689, de 3 de maio de 2023, conforme detalhamento a seguir:

- I) ID PCA no PNCP : 46377222000129-0-000003/2026;
- II) Data de Publicação no PNCP : 23/06/2025;
- III) Id do item no PCA: 33;
- IV) Classe/Grupo: 5810 - Equipamentos e componentes para segurança de comunicações;
- V) Identificador da Fatura Contratação: 93311-48/2026.

3. Contratações correlatas/interdependentes

Registra-se que não foi constatada contratações correlatas, ou seja, aquelas cujos objetos possuem semelhança entre si e podem ser adquiridos em conjunto para maior eficiência. Além disso, não se classifica com uma contratação interdependente já que não depende diretamente de outra para sua plena utilidade ou execução.

4. Descrição da necessidade

4.1 A coordenação das atividades relacionadas à tecnologia da informação na Secretaria da Fazenda e Planejamento do Estado de São Paulo (SEFAZ-SP) é realizada pela Diretoria de Tecnologia da Informação e Comunicação - DTIC conforme previsto no Decreto nº 69.182, de 18 de dezembro de 2024.

4.2 Essa mesma legislação prevê que a Diretoria de Tecnologia da Informação e Comunicação – DTIC é o responsável, no âmbito da Secretaria: gerenciar os recursos e os meios necessários para o desenvolvimento e implantação de soluções em serviços e produtos de TIC, envolvendo a contratação e aquisição de produtos e serviços de TIC; realizar a gestão contratual e financeira de todas as contratações de TIC; realizar a gestão técnica das soluções de TIC implantadas, em consonância com as diretrizes da Secretaria.

4.3 Por meio do Processo SF nº SFP-PRC-2022/06848, Pregão Eletrônico NC nº 10/2022, contrato 31338-SAAC-00086-2022, esta Secretaria adquiriu da empresa DINAMO NETWORK - SERVIÇOS, DESENVOLVIMENTO E PARTICIPAÇÃO EM CONSÓRCIOS OU EMPRESA S.A uma Solução de

Hardware Security Module – HSM, incluindo Aquisição de Hardware, Software e Licenças Integrados para a Solução; Serviços de Instalação, Configurações, Testes e Documentação da Solução; Suporte Técnico; Treinamento e Banco de Horas.

4.4 A SEFAZ-SP possui atualmente 4 (quatro) equipamentos HSM do fabricante Dinamo. Dois equipamentos estão hospedadas no Datacenter de São Paulo e 2 estão no datacenter de Campinas.

4.5 O objetivo desta solicitação é contratar uma nova Solução de Hardware Security Module – HSM, já que os equipamentos atuais irão ter o fim da vida útil em 26/09/2026, não havendo mais possibilidade de prorrogar os serviços contínuos de Suporte Técnico, Manutenção com reposição de Hardware e Atualização de Software para Solução de HSM.

4.6 Para garantir um alto nível de segurança no armazenamento das chaves criptográficas privadas faz-se necessária a contratação de novos HSMS.

5. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia da Informação e Comunicação - DTIC	Eudes Argeo Cherighim

6. Necessidades de Negócio

O uso da solução de HSM está relacionado a todas áreas de negócio da SEFAZ-SP que usam nas suas aplicações certificados digitais e consequentemente requerem o armazenamento das chaves criptográficas em um ambiente seguro.

7. Necessidades Tecnológicas

7.1	REQUISITOS GERAIS
7.1.1	A solução descrita neste item deverá ser entregue pela CONTRATADA: na Sede da SEFAZ à Av. Rangel Pestana, 300, São Paulo/SP , e na Regional de Campinas da SEFAZ localizada à Av. Dr. Alberto Sarmiento Campinas, Nº 4, Campinas-SP .
7.1.2	O prazo para a entrega dos equipamentos no endereço acima referido é de 60 (sessenta) dias corridos , contados da data da assinatura do contrato.
7.1.3	Deverão ser fornecidos hardware, software e licenças em quantidade suficiente para atender a todos os requisitos listados neste Memorial Descritivo.
7.1.4	A entrega de equipamentos deverá ser realizada sempre em dias úteis, entre as 09h e 12h ou entre 14h e 16h, sendo a SEFAZ avisada com uma antecedência mínima de 02 (dois) dias úteis quanto à data da entrega.

7.1.5	<p>Deverão ser entregues:</p> <ul style="list-style-type: none"> - 01 (um) equipamento na Sede da SEFAZ, em São Paulo/SP; - 01 (um) equipamento na Regional de Campinas, em Campinas-SP.
7.1.6	<p>A CONTRATADA deverá montar em rack, instalar em local indicado pela SEFAZ e energizar, todos os equipamentos fornecidos de forma a ser possível certificar que todos os itens inicialmente previstos foram entregues.</p>
7.1.7	<p>O TERMO DE RECEBIMENTO DEFINITIVO do ITEM – Aquisição de hardware, software e licenças integrados para a Solução, será emitido, em até 30 (trinta) dias da sua entrega, após a comprovação da conformidade dos produtos entregues com aqueles especificados e da entrega dos testes solicitados no subitem 7.3.1.</p>
7.2	<p>CARACTERÍSTICAS DA SOLUÇÃO HSM</p>
7.2.1	<p>Deverão ser fornecidos 02 (dois) equipamentos HSM, do mesmo fabricante, que atendam completamente todas as especificações.</p>
7.2.2	<p>Os equipamentos HSM serão definidos em grupos e segmentos distintos para utilização na rede da SEFAZ, funcionando em alta disponibilidade conforme especificado no subitem 7.6.</p>
7.2.3	<p>Equipamentos que operam exclusivamente com tokens/smartcards para proverem autenticação e funções de segurança do HSM, deverão ser entregues no mínimo 10 (dez) <i>tokens</i> ou <i>smartcards</i>, para cada equipamento HSM fornecido.</p>
7.2.4	<p>Para cada HSM fornecido deverá ser entregue no mínimo 01 (uma) mídia apropriada para o armazenamento do backup das chaves do equipamento ou permitir o backup através da rede de dados utilizando mecanismos seguros de criptografia e recuperação. Serão aceitos sistemas de backup tanto em hardware como por software. Quando o equipamento suportar o backup em hardware, todos os componentes necessários para utilização desse método deverão ser ofertados.</p>
7.2.5	<p>No caso de equipamentos que operam exclusivamente com tokens /smartcards para autenticação, deverão ser fornecidos no mínimo 02 (dois) componentes de hardware capazes de permitir que usuários fisicamente localizados no prédio Sede da SEFAZ em São Paulo-Capital possam autenticar-se nos equipamentos HSMs hospedados na Regional de Campinas para todas as atividades onde a autenticação “M de N” estiver habilitada, inclusive quando a autenticação de duplo fator (<i>token</i> ou <i>smartcard</i> e senha do usuário) for utilizada.</p> <p>O mecanismo de comunicação adotado deverá utilizar criptografia e ser capaz de utilizar a infraestrutura de comunicação existente entre os sites através de conectividade TCP/IP.</p>

7.2.6	Os hardwares e softwares ofertados na composição deste item não deverão estar listados como “End Of Sale” ou “End Of Life” por seus respectivos fabricantes até a data da abertura das propostas. No mínimo 5 anos após a assinatura do contrato para declarar “End of Support”
7.2.7	Deverão ser fornecidos hardware, software e licenças em quantidade suficiente para atender plenamente a todos os requisitos listados neste edital.
7.2.8	Os equipamentos deverão ser novos, sem uso, e ser produzidos em série na data da abertura das propostas.
7.2.9	Todo licenciamento necessário para o atendimento aos requisitos deste edital deverá ser na modalidade perpétua.
7.2.10	O módulo criptográfico dos HSM fornecidos deverá possuir certificado ICP-Brasil MCT-7 NSH-2 (ou superior) ou FIPS 140-2 Level 3. Não sendo aceitos equipamentos que “suportem”, “sejam baseados em”, “estejam em processo de certificação” ou qualquer expressão que implique que algum componente não esteja efetivamente certificado na norma ICP-Brasil MCT-7 NSH-2 (ou superior) ou FIPS 140-2 Level 3 na data da abertura das propostas.
7.2.11	<p>A certificação acima mencionada deverá ser verificável através de acesso ao site do NIST (<i>National Institute of Standards and Technology</i>) para o certificado FIPS.</p> <p>Para equipamentos com certificado ICP-Brasil, a certificação deverá ser verificável através de acesso ao site do ITI ou documento comprobatório emitido pelo Instituto.</p>
7.3	TESTES DO EQUIPAMENTO
	<p>A CONTRATADA deverá fornecer documento com o resultado dos testes relacionados abaixo para COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS SOLICITADAS. Os testes para COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS SOLICITADAS devem ser executados em ambientes de teste da CONTRATADA, sem nenhuma participação da SEFAZ e sem nenhum fornecimento de hardware/software para sua execução.</p> <p>A não apresentação do documento impede a emissão do TERMO DO RECEBIMENTO DEFINITIVO, conforme subitem 7.1.7.</p> <p>O documento deverá conter, além dos procedimentos, ferramentas e resultados, o teste mínimo dos seguintes itens:</p> <ol style="list-style-type: none"> Realização de no mínimo 500 (quinhentas) operações de assinatura por segundo com chaves RSA com tamanho de 2048 bits através do módulo criptográfico via hardware;

7.3.1	<p>b. Suporte e execução de operações com os seguintes algoritmos padrões de mercado, de domínio público:</p> <ul style="list-style-type: none"> • Chaves Assimétricas via RSA (1024-8192 bit), Elliptic Curve Digital Signature Algorithm (ECDSA) Elliptic-curve Diffie–Hellman (ECDH) • Assinatura digital via RSA (1024-8192 bit), Elliptic Curve Digital Signature Algorithm (ECDSA) Elliptic-curve bit) • Chaves Simétricas via 3DES (double & triple key lengths), AES; • Hash Digest via SHA-1, SHA-2, SHA-3; • Códigos de autenticação via HMAC. <p>c) Integração e compatibilidade na criptografia de Banco de Dados SQL SERVER (Enterprise) , usando o recurso Extensible Key Management - EKM da Microsoft, no mínimo algoritmo RSA (2048 bits) e AES (256 bits) em chaves simétricas e assimétricas para as seguintes versões:</p> <p>Management – EKM, nas seguintes versões:</p> <ul style="list-style-type: none"> - SQL SERVER 2019 CU28 e versões superiores. - SQL SERVER 2022 CU14 e versões superiores. <p>d) Integração e compatibilidade na criptografia de Banco de Dados Oracle, no mínimo algoritmo RSA (2048 bits) e AES (256 bits) em chaves simétricas e assimétricas para as seguintes versões:</p> <ul style="list-style-type: none"> - Oracle Advanced Security 19c ou superior. <p>e) Integração com o serviço de certificado digital da Microsoft CA (ADCS), incluindo geração, importação e exportação de chaves, bem como emissão de LCR (Lista de Certificados Revogados) e emissão de certificados digitais utilizando as chaves criptográficas das Autoridades Certificadoras presentes no HSM.</p>
7.3.1.1	O prazo para realização dos testes e apresentação do documento de resultados será de, no máximo, 15 (quinze) dias corridos a partir da assinatura do contrato.
7.3.2	O documento de resultado dos testes será analisado pela equipe técnica da SEFAZ quanto aos procedimentos, ferramentas, protocolos e resultados dos testes de forma a comprovar o atendimento de todas as especificações deste Termo de Referência.
7.3.2.1	O prazo para análise do documento pela equipe técnica da SEFAZ será de, no máximo, 05 (cinco) dias úteis.

7.4	Características físicas e de desempenho a serem atendidas por todos os equipamentos que compõe a solução
7.4.1	Cada HSM a ser fornecido deverá ser um equipamento do tipo <i>appliance</i> , ou seja, módulo projetado especificamente para atender a solução, com sistema operacional otimizado para esse fim e instalável em rack padrão 19", assim como todas as peças necessárias para esta instalação/fixação física em rack.
7.4.2	Cada equipamento fornecido não deverá ocupar mais do que 2U de espaço em rack a ser fornecido pela SEFAZ.
7.4.3	Cada equipamento fornecido deverá possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação.
7.4.4	Cada equipamento fornecido deverá possuir fonte de alimentação redundante 110/220 v (AC).
7.4.5	O plugue deve ser padrão ABNT NBR 14136 ou NEMA 5-15 com adaptador para ABNT NBR 14136. Caso seja necessária a substituição, deverá ser realizada pela CONTRATADA sem prejuízo de garantia e suporte.
7.4.6	O equipamento deverá ser resistente à violação física (<i>tamper resistant</i>), com destruição das chaves armazenadas em caso de violação física.
7.4.7	Cada HSM deverá possuir interface de rede Gigabit Ethernet 1000Base-T.
7.4.8	Cada HSM deverá possuir aceleração criptográfica através de processador criptográfico dedicado.
7.4.9	Cada HSM deverá ser capaz de armazenar no mínimo 500 chaves RSA de 2048 bits on-board ou em dispositivo de hardware seguro.
7.4.10	Cada HSM deverá gerar chaves RSA "on-board", isto é, de forma interna ao processador criptográfico dedicado.
7.4.11	Cada HSM deverá gerar números randômicos de acordo com ANSI X9.17 anexo C ou padrão sucessor.
7.4.12	Cada HSM deverá fazer assinatura digital, criptografia e decriptografia em hardware no processador criptográfico.
7.4.13	Cada HSM deverá ser entregue com todos os recursos necessários para realizar no mínimo 500 operações de assinatura por segundo, chaves RSA com tamanho de 2048 bits através do módulo criptográfico via hardware.

7.4.14	Cada HSM deverá permitir a conexão simultânea de no mínimo 100 (cem) clientes requisitando operações de assinatura digital.
7.4.15	Para cada HSM deverá ser possível a criação de no mínimo 10 partições para armazenamento das chaves criptográficas. Também serão aceitos HSMs que não são estruturados em partições, mas permitem a segregação (mínimo de 10), o controle e acesso das chaves criptográficas armazenadas.
7.5	FUNCIONALIDADES GERAIS
7.5.1	A solução deverá possuir API's PKCS#11, Microsoft CAPI e CNG, JAVA (JCA/JCE), OpenSSL e Software cliente a ser instalado nos servidores. Software cliente refere-se ao componente instalado em um servidor, computador ou aplicação que precisa interagir com o HSM para realizar operações criptográficas seguras, como: geração de chaves; assinatura digital; criptografia/descriptografia; armazenamento e uso seguro de chaves criptográficas.
7.5.2	Juntamente com as licenças de uso deverá ser fornecido o conjunto de mídias ou certificado de aquisição correspondente aos softwares da solução, de forma a permitir a instalação da aplicação em inglês ou português.
7.5.3	O software cliente da solução que fará a comunicação entre os servidores e os HSMs devem oferecer suporte a AAA (<i>Authentication, Authorization and Accounting</i>), Balanceamento de Carga, <i>Failover</i> e HA (<i>High Availability</i>) e ser transparente para as aplicações hospedadas nos servidores (software cliente transparente), não requerendo alterações por parte das aplicações já instaladas nos servidores.
7.5.4	A conexão entre o HSM e o Software cliente da solução a ser instalado nos servidores deve ser protegida através de conexão cifrada SSL 128 bits ou algoritmo proprietário de segurança, com autenticação mútua e cadeia de confiança entre os dispositivos.
7.5.5	<p>Cada HSM deverá ter os seguintes algoritmos de criptografia e <i>hash</i> padrões de mercado, de domínio público:</p> <ul style="list-style-type: none"> • Chaves Assimétricas via RSA (1024-8192 bit), Elliptic Curve Digital Signature Algorithm (ECDSA) Elliptic-curve Diffie–Hellman (ECDH) • Assinatura digital via RSA (1024-8192 bit) • Chaves Simétricas via 3DES (double & triple key lengths), AES; • Hash Digest via SHA-1, SHA-2, SHA-3. • Códigos de autenticação via HMAC.
7.5.6	Cada HSM deverá gerar backups das chaves em hardware apropriado (HSM, <i>token</i> ou <i>smartcard</i>) certificado ICP-Brasil MCT-7 NSH-2 (ou superior) ou FIPS 140-2 Level 3 a prova de violação, ou permitir o <i>backup</i> através da rede de dados utilizando mecanismos seguros de criptografia e recuperação.

5.5.7	No caso de equipamentos que operam exclusivamente com tokens /smartcards para autenticação, cada HSM deverá possuir interface para dispositivo do tipo teclado (PIN PAD) ofertado junto à solução para cada uma das localidades, com criptografia incorporada ou entrada USB para teclado diretamente no HSM, provendo autenticação de duplo fator de segurança, como <i>smartcard</i> , <i>token</i> etc., a fim de evitar que a senha trafegue por ambiente desprotegido.
7.5.8	O software cliente da solução que fará a integração entre os servidores e os HSMs deve oferecer suporte à instalação nos seguintes sistemas operacionais: - Windows Server 2016 e versões superiores; - Red Hat Linux 8.0 ou superior.
7.6	Redundância a Falhas e Alta Disponibilidade
7.6.1	Os equipamentos HSM deverão operar em modo de balanceamento de carga (<i>load balancing</i>), permitindo que as requisições sejam balanceadas entre os equipamentos configurados no grupo.
7.6.2	Os equipamentos HSM deverão operar em modo de alta disponibilidade, em modos ativo-ativo e ativo-passivo. Caso algum dos equipamentos venha a falhar, os outros do grupo deverão continuar as operações de forma transparente às aplicações.
7.6.3	A solução fornecida deverá ser capaz de ter seu desempenho aumentado através da agregação de novos equipamentos HSM do mesmo fabricante, de forma que a capacidade conjunta destes seja agregada.
7.6.4	Deverão ser formados pares redundantes, dispostos em sites distintos de forma a manter a alta disponibilidade em caso de queda de um dos sites.
7.7	Gerenciamento
7.7.1	O gerenciamento da solução deverá ser feito através de software cliente para Windows e/ou acesso através de navegador Web. Ambos os canais deverão ser protegidos por criptografia.
7.7.2	O HSM deverá possuir <i>comand line interface</i> acessível via console física ou remotamente através do protocolo SSH (secure shell).
7.7.3	No caso de equipamentos que operam exclusivamente com tokens /smartcards para autenticação, o HSM deverá implementar proteção por autenticação “M de N”, através de dispositivo com chip criptográfico (

	<i>smartcard, token</i> etc.), ofertado junto à solução, para atividades administrativas , recuperação de chaves criptográficas e recuperação de backups.
7.8	LOGS
7.8.1	Deve possuir capacidade de armazenamento de logs do sistema, para identificação de funcionamento dos principais componentes de gerenciamento e armazenar logs de auditoria, para registro de todas as atividades dos usuários na solução.

8. Demais requisitos necessários e suficientes à escolha da solução de TIC

8.1 Serviços de instalação, configuração, testes e documentação da Solução.

8.1.1	REQUISITOS GERAIS
8.1.1.1	Os serviços descritos neste item deverão ser prestados na Av. Rangel Pestana, 300, São Paulo/SP, e na Regional de Campinas da SEFAZ localizada à Av. Dr. Alberto Sarmento Campinas, Nº 4, Campinas-SP.
8.1.1.2	A CONTRATADA será responsável, perante a SEFAZ-SP, por todos os serviços descritos neste item.
8.1.1.2.1	Os serviços de instalação física, configuração, testes e documentação, deverão ser executados por equipe técnica da CONTRATADA.
8.1.1.3	Eventuais custos com alimentação, transporte e estadia dos profissionais envolvidos na prestação dos serviços descritos neste item correrão por conta da CONTRATADA.
8.1.1.4	A CONTRATADA deverá montar os equipamentos em rack e instalar em local definitivo a ser indicado pela SEFAZ.
8.1.2	Prazo de execução
8.1.2.1	O prazo total para a conclusão dos serviços de instalação, configuração, testes e documentação da solução não poderá ultrapassar 120 (cento e vinte) dias corridos, contados da assinatura do contrato.
8.1.3	Fases da implantação – A implantação da solução deverá contemplar as seguintes fases:
8.1.3.1	Planejamento
8.1.3.1.1	Na etapa de Planejamento, a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano testes, a localização dos equipamentos na arquitetura da rede da SEFAZ-SP, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Deverão ser consideradas as janelas de manutenção da SEFAZ-SP, plano de rollback e o escopo definido. Os responsáveis técnicos da SEFAZ-SP acompanharão e aprovarão o planejamento.
8.1.3.2	Documentação do projeto – Deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato e quantidade a serem acordados entre as partes e nos momentos especificados:
8.1.3.2.1	Cronograma: ao final do planejamento, a CONTRATADA deverá, em conjunto com representantes do Departamento de Tecnologia da Informação e Comunicação (DTIC) da SEFAZ-SP, elaborar e apresentar um cronograma detalhado, contendo todas as fases e datas necessárias para disponibilizar a solução para uso, inclusive treinamentos, observados os prazos previstos na proposta comercial e os processos internos da SEFAZ-SP (gerenciamento de mudanças).
8.1.3.2.2	Plano de Requisitos de Infraestrutura: a CONTRATADA, antes de iniciar a execução das instalações deverá levantar as necessidades de infraestrutura necessárias para instalação da configuração (espaço em rack, energização, refrigeração, tipo de conectorização, entre outros) e apresentá-las através de um documento denominado “Plano de Requisito de Infraestrutura”. Caso seja necessário, uma vistoria deverá ser realizada pela CONTRATADA.
8.1.3.2.3	Plano de Implementação: a CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar uma documentação técnica denominada “Plano de Implementação”, fundamentando todas as configurações que serão realizadas
8.1.3.2.4	Assinatura digital com e-CNPJ A CONTRATADA será responsável pela integração de pelo menos 1 (uma) aplicação através de software cliente transparente para a aplicação - conforme subitem 8.5.3 - a qual permita utilizar o e-CNPJ armazenado nos HSMS para a assinatura digital de arquivos e documentos quando solicitados por aplicação autorizada.

	<p>Assinatura de Código de Software</p> <p>A CONTRATADA será responsável pela geração de template (perfis criptográficos onde constem todos os detalhes que vão compor o certificado, conforme padrão X-509 mais recente) e CSR (Certificate Signing Request) de assinatura de código em HSM e integração com o SDK de cada fabricante (SDK Microsoft para Windows 10 ou posterior e Java JDK 1.8 ou superior), a ser utilizado para assinar o código fonte de até dois aplicativos desenvolvidos pela SEFAZ, ou utilizar-se de solução proprietária segura para o mesmo fim. A integração para assinatura de código deverá ser programada ou customizada para utilizar autenticação “M de N”, a critério da SEFAZ.</p> <p>Criptografia de Banco de Dados</p> <p>A CONTRATADA será responsável pela geração de CSR para certificado de criptografia de banco de dados, assim como a integração e compatibilidade na criptografia de Banco de Dados SQL SERVER (Enterprise), usando o recurso Extensible Key Management - EKM da Microsoft, no mínimo algoritmo RSA (2048 bits) e AES (256 bits) em chaves simétricas e assimétricas para as seguintes versões:</p> <p>Management – EKM, nas seguintes versões:</p> <ul style="list-style-type: none"> - SQL SERVER 2019 CU28 e versões superiores. - SQL SERVER 2022 CU14 e versões superiores. <p>Integração e compatibilidade na criptografia de Banco de Dados Oracle, no mínimo algoritmo RSA (2048 bits) e AES (256 bits) em chaves simétricas e assimétricas para as seguintes versões:</p> <ul style="list-style-type: none"> - Oracle Advanced Security 19c ou superior. <p>Desta forma, provendo a criptografia dos dados armazenados no banco de dados.</p> <p>Integração com serviço Microsoft AD CS</p> <p>Integração com o serviço de certificado digital da Microsoft CA (ADCS), incluindo geração, importação e exportação de chaves, bem como emissão de LCR (Lista de Certificados Revogados) e emissão de certificados digitais utilizando as chaves criptográficas das Autoridades Certificadoras presentes no HSM.</p> <p>A aquisição de todos os certificados digitais gerados na migração é de responsabilidade da SEFAZ.</p>
8.1.3.2.5	<p>Plano de Testes: A CONTRATADA deverá entregar uma documentação técnica denominada “Plano de Testes”, de forma a garantir que todas as características exigidas neste edital tenham sido satisfeitas. Deve incluir no mínimo:</p> <ul style="list-style-type: none"> • Teste das funcionalidades da solução (assinatura de Arquivo com certificado CNPJ, assinatura de código java, assinatura de código .net, Integração banco de dados SQL Server e Oracle com HSM, usando no mínimo AES (256 bits), integração com serviço Microsoft AD CS e backup; • Teste de alta disponibilidade (balanceamento de carga); • Teste de qualidade (conectividade de interface de rede e fontes de energia atuando em redundância); • Teste de desempenho. (executar 500 operações de assinatura por segundo, com chave RSA de tamanho de 2048 bits).
8.1.3.2.6	<p>Guia Rápido de Utilização: A CONTRATADA deverá fornecer uma documentação técnica denominada “Guia Rápido de Referência” voltada para os usuários, customizada para utilização mais comum da solução.</p>
8.1.3.2.7	<p>Toda a documentação será analisada pela SEFAZ e deverá ser complementada pela CONTRATADA caso seja solicitado.</p>
8.1.3.2.8	<p>Toda adição, remoção e/ou modificação de equipamentos e serviços no ambiente de produção da SEFAZ deverá passar por avaliação e aprovação do DTIC da SEFAZ, devendo a CONTRATADA fornecer todas as informações necessárias para a avaliação e aprovação das mudanças propostas.</p>
8.1.3.2.9	<p>Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e cumprimento dos prazos pactuados.</p>
8.1.3.3	<p>Instalação física dos equipamentos</p>
8.1.3.3.1	<p>Os requisitos da instalação física dos equipamentos estão especificados no subitem 8.4.</p>
8.1.3.4	<p>Configuração</p>
8.1.3.4.1	<p>A configuração da solução deverá ser realizada em conformidade com as recomendações do fabricante.</p>
8.1.3.4.2	<p>Após a configuração deverão ser realizadas verificações pela equipe da CONTRATADA, acompanhada por representantes da SEFAZ-SP, para atestar a perfeita conformidade da solução configurada com os requisitos descritos neste Memorial Descritivo.</p>
8.1.3.5	<p>Etapas de testes e de funcionamento experimental</p>
8.1.3.5.1	<p>Todos os componentes implantados deverão ser testados de forma a validar o pleno atendimento dos requisitos especificados neste Memorial Descritivo.</p>
8.1.3.5.2	<p>Nesta fase, a CONTRATADA deverá demonstrar que todas as funcionalidades da solução especificadas neste Memorial Descritivo existem e estão operacionais.</p>

8.1.3.5.3	A CONTRATADA deverá emitir relatórios e validar os procedimentos de operação das assinaturas digitais e contingência da solução.
8.1.3.5.4	Ao final da Etapa de Testes e de Funcionamento Experimental, após a realização de ajustes de configuração necessários, a solução deverá funcionar em perfeitas condições e na forma esperada pela SEFAZ-SP por um período mínimo de 3 (três) dias úteis, sem a necessidade de realização de mudanças de configuração ou qualquer outro tipo de ajuste ou procedimento, como condição para homologação do funcionamento e da estabilidade da solução em ambiente de teste.
8.1.3.5.4.1	Caso surja a necessidade de realização de algum ajuste de configuração ou de qualquer outro tipo de ajuste ou procedimento, seja física ou lógica, durante o período de 3 (três) dias úteis referido no subitem 8.1.3.5.4 acima, ficará a critério da SEFAZ-SP decidir se o referido prazo deverá ser interrompido, reiniciando-se a partir da finalização do novo ajuste.
8.1.3.6	Validação do funcionamento em ambiente de produção
8.1.3.6.1	Após a Fase Funcionamento Experimental, será realizada a ativação da solução em ambiente de produção. A solução deverá permanecer em operação ininterrupta por um período de no mínimo 5 (cinco) dias úteis, sem necessidade de aplicação de quaisquer mudanças de configuração ou qualquer outro tipo de ajuste ou procedimento, como condição para homologação do funcionamento e da estabilidade da solução em ambiente de produção.
8.1.3.6.1.1	Surgindo a necessidade de realização de algum ajuste de configuração ou de qualquer outro tipo de ajuste ou procedimento, seja física ou lógica, durante o período de 5 (cinco) dias úteis referido no subitem 8.1.3.6.1 acima, ficará a critério da SEFAZ-SP decidir se o referido prazo deverá ser interrompido, reiniciando-se a partir da finalização do novo ajuste.
8.1.3.6.2	A solução, após a sua validação no ambiente de produção, passará a fazer parte da infraestrutura ativa da SEFAZ-SP.
8.1.3.7	Documentação Final
8.1.3.7.1	Após a implantação, a CONTRATADA deverá entregar a documentação técnica final do projeto, denominada “Documentação Final”, contendo no mínimo: documentação da implementação realizada, documentação da arquitetura adotada, descrição do esquema de redundância implementada, instruções para backup/restauração, cópia das configurações realizadas em todos os elementos com comentários, número serial dos produtos entregues, lista detalhada dos produtos entregues.
8.1.3.7.2	A Documentação Final poderá incluir outras informações que a SEFAZ-SP ou a CONTRATADA julgarem importantes para o registro fiel de como a solução foi implementada.
8.1.3.7.3	O prazo para a entrega da Documentação Final está incluído no prazo total referido no subitem 8.1.2.1
8.1.3.8	Finalização e aceitação definitiva
8.1.3.8.1	A solução implantada será aceita definitivamente se e somente se houver comprovação de que todos os requisitos técnicos especificados neste Memorial Descritivo tenham sido atendidos. Tal comprovação far-se-á em até 10 (dez) dias úteis após a entrega da Documentação final do Projeto, mediante observação direta das características dos equipamentos, verificação do funcionamento adequado das funções especificadas, consulta à documentação técnica fornecida e constatação da execução dos serviços de instalação, configuração, testes e documentação, conforme os termos deste Memorial Descritivo.
8.1.3.8.2	O TERMO DE RECEBIMENTO DEFINITIVO do ITEM 8.1 – Serviços de instalação, configuração, testes e documentação da Solução, será emitido, em até 5 (cinco) dias úteis, após a comprovação referente ao subitem 8.1.3.8.1.
8.1.3.8.3	A data de assinatura do termo referido no subitem 8.1.3.8.2 deste Memorial Descritivo constituirá o marco inicial da vigência do ITEM 8.2 - Prestação de serviços continuados de suporte técnico, manutenção com reposição de hardware e atualização de software, pelo período de 15 (quinze) meses.

8.2 Prestação de serviços continuados de suporte técnico, manutenção com reposição de hardware e atualização de software, para a Solução, pelo período de 24 (vinte e quatro) meses, prorrogáveis até o limite de 120 (cento e vinte) meses.

8.2.1	Os serviços de atualização de software consistem em disponibilizar, durante a vigência do contrato, as novas versões e os novos “releases” dos softwares da solução, sem quaisquer ônus para a Sefaz, no prazo máximo de 30 (trinta) dias após o lançamento da versão ou “release” no mercado.
8.2.2	Consideram-se novas versões de um mesmo produto de software as atualizações para consolidação de correções de manutenção e de “bugs” anteriores a elas e/ou inclusão de novos recursos, identificadas geralmente por variações na parte à esquerda do ponto decimal na identificação do software.

8.2.3	Consideram-se novos “releases” (lançamentos) as atualizações de menor monta dentro de uma mesma versão de software, identificados geralmente por variações na porção à direita do ponto decimal na identificação do software.
8.2.4	Eventuais custos com alimentação, transporte e estadia dos profissionais envolvidos na prestação dos serviços correrão por conta da CONTRATADA.
8.2.5	Os serviços deverão ser prestados em dias úteis, sábados, domingos e feriados, em regime 24x7 (vinte e quatro horas por dia e sete dias por semana).
8.2.6	Detalhamento do Suporte Técnico
8.2.6.1	O Suporte Técnico será prestado nas modalidades Remota e Local. Nenhum chamado poderá ser encerrado sem aprovação da CONTRATANTE.
8.2.6.2	O Suporte Técnico Remoto deverá ser prestado em horário 24 x 7 (vinte e quatro horas por dia e sete dias por semana), incluindo dias úteis, sábado, domingo e feriados, através de telefone, correio eletrônico e Internet (qualquer serviço acessível via navegador através da internet), sem limite de horas, para todos os componentes (software e hardware) da solução, abrangendo:
a.	<ul style="list-style-type: none"> • Suporte corretivo: correção de “bugs” e/ou falhas, e quaisquer atividades que tenham por finalidade restabelecer o normal funcionamento da solução, tanto na sua parte de hardware quanto na de software.
b.	<ul style="list-style-type: none"> • Suporte preventivo: atualização dos softwares, por meio de patches; alerta e correção de possíveis incompatibilidades detectadas; recomendação de configurações consoante às melhores práticas.
c.	<ul style="list-style-type: none"> • Esclarecimento de dúvidas de natureza técnica relativas aos equipamentos e ao seu ambiente de operação, bem como sobre a instalação, configuração, manutenção e operacionalização dos equipamentos, e a instalação, desinstalação e atualização de software.
d.	<ul style="list-style-type: none"> • Dúvidas e suporte sobre regras e funcionamento gerais, além da inclusão de recursos correlacionados a proteção e uso das chaves criptográficas utilizadas pela solução de HSM da Sefaz.
e.	<ul style="list-style-type: none"> • Avaliação dos registros de desempenho dos equipamentos e análise de eventuais erros identificados, quando solicitadas pela Sefaz, e proposição de ajustes para melhorar o desempenho, bem como emissão de parecer técnico.
8.2.6.3	A CONTRATADA deverá possuir endereço de correio eletrônico (e-mail) e serviços de Central de Atendimento que disponibilize, ao menos, um número de telefone de São Paulo, Capital (ligação local), ou 0800 (ligação gratuita), que funcionarão como canal para o suporte técnico remoto durante a vigência do contrato.
8.2.6.4	O prazo para início do atendimento remoto não poderá ultrapassar 5 (cinco) minutos na fila de espera do atendimento telefônico, ou 1 (uma) hora para resposta via e-mail.
8.2.6.5	Para atendimentos de Suporte Técnico Remoto, o tempo máximo de fechamento com resolução das questões que levaram à abertura do chamado ou sugestão de medida de contorno que atenda às necessidades da Sefaz e seja por esta aprovada não deve exceder 02 (dois) dias úteis, exceto nos seguintes casos:

a.	O encerramento do chamado depende do desenvolvimento e/ou disponibilização de "Patch", funcionalidade ou nova versão dos softwares envolvidos por parte de seus respectivos fabricantes;
b.	A finalização do atendimento depende de retorno do fabricante da solução para um chamado aberto pela CONTRATADA junto ao fabricante, desde que a CONTRATADA não esteja em falta com as informações e/ou procedimentos solicitados pelo fabricante;
c.	A finalização do atendimento depende de informações que devem ser providas pela Sefaz.
8.2.6.5.1	O prazo para o atendimento de Suporte Técnico Remoto nas situações de exceção acima relacionadas será fixado, caso a caso, pela Sefaz de acordo com o grau de criticidade, isto é, se o problema causa perda ou paralisação dos serviços.
8.2.6.6	O Suporte Técnico Local deverá ser prestado em horário 24 x 7 (vinte e quatro horas por dia e sete dias por semana), incluindo dias úteis, sábado, domingo e feriados, abrangendo todas as atividades do subitem 8.2.6.2 Suporte Técnico Remoto e que requeiram a presença de técnico especialista no local do problema.
8.2.6.7	Os prazos para início do Suporte Técnico Local serão estabelecidos de acordo com o grau de criticidade da situação que motivar o chamado, o qual será informado pela Sefaz quando da abertura do chamado, sendo considerado:
a.	<ul style="list-style-type: none"> • CRÍTICO: O problema causa perda ou paralisação total dos serviços da solução. O trabalho não pode ter sequência razoável, a operação passa a ser crítica para o negócio e a situação constitui uma emergência. Atendimento local até 4 (quatro) horas corridas da abertura do chamado.
b.	<ul style="list-style-type: none"> • MÉDIO: O problema causa uma grave perda de funcionalidade. Não está disponível nenhuma alternativa aceitável, mas as operações podem continuar ainda que de modo restrito. Atendimento local até 10 (dez) horas corridas da abertura do chamado.
c.	<ul style="list-style-type: none"> • NORMAL: O problema causa perda de funcionalidade de pequena gravidade. O impacto constitui uma inconveniência, a qual pode requerer uma solução alternativa para restabelecer a funcionalidade normal. Atendimento local até 1 (um) dia útil da abertura do chamado.
8.2.6.8	No atendimento de Suporte Técnico Local classificado como CRÍTICO ou MÉDIO, a equipe da CONTRATADA responsável pelo atendimento deverá permanecer disponível no local até que uma das seguintes condições seja alcançada:
a.	<ul style="list-style-type: none"> • O problema seja definitivamente resolvido;
b.	<ul style="list-style-type: none"> • Medida de contorno tenha sido aplicada pela CONTRATADA e aprovada pela equipe técnica da Sefaz, de forma que o serviço retorne ao seu funcionamento normal.
c.	<ul style="list-style-type: none"> • Reposição antecipada de hardware junto ao fabricante seja acionada, nas condições especificadas no subitem 8.2.7 - Detalhamento da Manutenção Incluindo Reposição Antecipada de Hardware deste Memorial Descritivo.
8.2.7	Detalhamento da Manutenção incluindo Reposição Antecipada de Hardware
8.2.7.1	

	Os serviços de manutenção devem garantir o funcionamento sem erros da solução de HSM da Sefaz, em conformidade com os padrões de uso e de segurança e recomendações do fabricante.
8.2.7.2	Os serviços de manutenção incluem a reposição, sob responsabilidade da CONTRATADA e sem ônus adicionais para a Sefaz, de hardware que venha a se revelar defeituoso.
8.2.7.3	A Sefaz poderá solicitar verificação periódica semestral da solução, a qual incluirá testes, medições e autodiagnóstico aplicados com risco controlado, quanto à integridade e ao sigilo das informações.
8.2.7.3.1	Caso sejam encontradas divergências em relação aos padrões de uso e de segurança e recomendações do fabricante, a CONTRATADA deverá propor, por meio de relatório analítico, medidas de adequação, as quais serão avaliadas pela Sefaz, cabendo a esta decidir sobre a viabilidade e a conveniência da execução das alterações propostas.
8.2.7.4	A reposição de hardware deve ser oferecida em horário 24 x 7 (vinte e quatro horas por dia e sete dias por semana), incluindo dias úteis, sábado, domingo e feriados.
8.2.7.5	A CONTRATADA deverá providenciar a reposição do hardware que venha a apresentar defeito por outro hardware com características e especificações técnicas iguais ou superiores.
8.2.7.5.1	O hardware de reposição deverá ser novo e estar em perfeitas condições de uso, a juízo da Sefaz.
8.2.7.5.2	Na reposição de hardware, a CONTRATADA deverá primeiramente enviar e instalar a peça de reposição, e somente após a comprovação de que a peça reposta restabeleceu a funcionalidade normal da solução, a CONTRATADA poderá retirar a peça defeituosa das dependências da Sefaz.
8.2.7.6	Caso o hardware de reposição apresentado seja diferente do hardware original, a Sefaz reserva-se o direito de não aceitar o hardware alternativo, sem interrupção dos prazos de reposição, especificados no subitem 8.2.7.8 a seguir.
8.2.7.7	Caso haja necessidade de substituição de produto que não seja mais fabricado em razão de evolução tecnológica, que não seja mais comercializado ou que, por qualquer motivo, não exista disponível para reposição, a CONTRATADA deverá, durante a vigência do contrato, proceder à substituição por produto tecnologicamente equivalente ou superior, compatível com a solução implantada na Sefaz.
8.2.7.8	Os prazos para reposição de hardware serão estabelecidos de acordo com o grau de criticidade da situação que motivar o chamado, o qual será informado pela Sefaz quando da abertura do chamado, sendo considerado:
a.	CRÍTICO: O problema causa perda ou paralisação total dos serviços da solução. O trabalho não pode ter sequência razoável, a operação passa a ser crítica para o negócio e a situação constitui uma emergência. A reposição deverá ocorrer em até 6 (seis) horas a partir da abertura do chamado, com o envio da peça de reposição antes da retirada da peça defeituosa.
b.	MÉDIO: O problema causa uma grave perda de funcionalidade. Não está disponível nenhuma alternativa aceitável, mas as operações podem continuar ainda que de modo restrito. A reposição deverá ocorrer até o dia útil seguinte ao da abertura do chamado, com o envio da peça de reposição antes da retirada da peça defeituosa.
c.	NORMAL: O problema causa perda de funcionalidade de pequena gravidade. O impacto constitui uma inconveniência, a qual pode requerer uma solução alternativa para restabelecer a funcionalidade normal. A reposição deverá ocorrer em até 2 (dois) dias úteis da abertura do chamado, com o envio da peça de reposição antes da retirada da peça defeituosa.

8.2.7.9	Na reposição de hardware, serão da responsabilidade exclusiva da CONTRATADA, sem custos adicionais para a Sefaz:
a.	O envio do hardware para a localidade na qual deverá ser instalado, Campinas ou São Paulo;
b.	O recolhimento do equipamento defeituoso, após concluída a reposição.

8.3 Treinamento

8.3.1	<p>Treinamento nas soluções fornecidas para o atendimento da Solução a que se refere o objeto desta contratação:</p> <p>Quantidade de alunos previstos: 4 (quatro)</p> <p>Carga horária mínima: 24 h (vinte e quatro)</p>
8.3.2	<p>O conteúdo programático dos treinamentos deverá estar anexo a proposta e deverão conter no mínimo: configuração, administração e utilização de todos os recursos solicitados no termo de referência assim como:</p> <p>Overview da Ferramenta; Conceitos de Criptografia; Conceitos de PKI, CA e AAA; Soluções de Arquitetura; Funcionalidades; Cartões de acesso; Regras de Segurança; Requerimentos para implementação; Operação em Alta Disponibilidade; Recuperação da solução em caso de recuperação de desastres; Backup; Configuração e Setup; Gerenciamento da console através de <i>shell</i>; Gerenciamento de políticas; Preparação e instalação dos <i>appliances</i>; Inicialização do HSM; Definição de partições; Rotina de boas práticas para a ativação; Instalação de software cliente da solução; Integração com PKCS#11 e Microsoft CAPI e CNG; Integração do HSM com Microsoft CA (ADCS); Integração com Microsoft SQL e Oracle; Assinatura Digital; Assinatura de Código; Importação e exportação de chaves criptográficas; Configuração e utilização do PIN PAD, se aplicável; Avaliação de performance dos equipamentos; Administração de usuários e reset de senhas; Melhores práticas de administração; <i>Troubleshooting</i> básico e avançado.</p> <p>Deverá apresentar uma visão arquitetônica da solução proposta, seu gerenciamento e monitoração.</p>
8.3.3	Os treinamentos deverão ser realizados na modalidade presencial ou remota (numa sala virtual). Cabe a SEFAZ a escolha da modalidade que será informada em até 30 (trinta) dias após a assinatura do contrato.
8.3.4	Os treinamentos devem ser em português para melhor aproveitamento.

9. Estimativa da demanda - quantidade de bens e serviços

Item	Descrição	Unidade	Quantidade
1	Aquisição de Solução de HSM – Hardware.	Unidade	2
	Aquisição de Solução HSM - Software e licenças integrados.	Unidade	2
2	Serviços de instalação, configuração, testes e documentação da solução	Unidade	1
3		Meses	24

	Prestação de serviços de suporte técnico, manutenção com reposição de hardware e atualização de software, pelo período de 24 (vinte e quatro) meses para toda a solução.		
4	Treinamento	Aluno	4

10. Levantamento de soluções

Há no mercado brasileiro fabricantes de HSMS e diversas empresas habilitadas para revender HSMS permitindo que haja um amplo nível de competitividade para aquisição da Solução.

11. Análise comparativa de soluções

Não se aplica.

12. Registro de soluções consideradas inviáveis

Não se aplica. Todos os fabricantes de HSM que atendam aos requisitos técnicos podem ofertar soluções a SEFAZ, não há escolha de marca.

13. Análise comparativa de custos (TCO)

Não se aplica.

14. Descrição da solução de TIC a ser contratada

Aquisição de Solução de Hardware Security Module – HSM, contemplando hardware, software, instalação /configuração/testes e documentação técnica, serviços continuados de suporte técnico, manutenção com reposição de hardware , atualização de software e treinamento.

15. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: O valor estimado da contratação será mantido em sigilo devido aos seguintes fatores: 1 - A não divulgação do orçamento tem por objetivo evitar que as propostas/lances gravitem em torno do orçamento fixado pela administração. Essa medida deve se mostrar particularmente eficaz quando houver a ocorrência de lances abertos, pois, sem as balizas dos outros licitantes e do orçamento da administração, o competidor deve, já nessa etapa, oferecer um preço realmente competitivo e dentro do limite de sua capacidade de executar a avença com uma lucratividade adequada. Amplia-se assim, a competitividade do certame e propicia-se propostas mais vantajosas a administração. Não se ouvida que determinados agentes do mercado participam de licitações e elaboram suas propostas sem analisar sua capacidade de honrá-la. Esses agentes, seja por não disporem de meios para tanto, seja por não estarem dispostos a arcar com as despesas daí decorrentes, simplesmente se baseiam no orçamento efetuado pela administração. Esse procedimento, contudo, é temerário porque as propostas podem não refletir a realidade econômica do licitante, redundando em dificuldades posteriores na execução contratual. Desta feita, a não divulgação do orçamento obriga os licitantes a efetivamente analisarem sua estrutura de custos para daí elaborarem suas propostas. Espera-se, pois, a apresentação de propostas mais realistas economicamente. 2 - Em relação a eventual violação do princípio da publicidade, explicitado no caput do art. 37 da Constituição Federal, deve-se lembrar o entendimento de que nenhum princípio constitucional é absoluto de forma que se deve buscar harmonizá-los na hipótese de eventual antagonismo entre dois princípios — no caso o da publicidade em contraposição aos da eficiência e da economicidade. Nesse contexto de ponderação de princípios, entende-se estar justificada a ausência temporária da divulgação do orçamento, pois amparada no princípio da busca da melhor proposta pela administração. Logo as principais razões do princípio da publicidade estarão atendidas, pois será garantida a transparência do procedimento licitatório com a divulgação do orçamento ao final do certame. Assim sendo, busca-se através do orçamento sigiloso a majoração da assertividade pela Administração, na escolha da contratada que sabendo dos riscos e complexidade da obra, objeto ou serviço, apresente proposta dentro da sua realidade para que tenha capacidade de honrar os compromissos assumidos na fase licitatória. Desta forma e por todo justificado anteriormente, informamos aos Licitantes que o ORÇAMENTO PREVIAMENTE ESTIMADO PARA A CONTRATAÇÃO SERÁ TORNADO PÚBLICO APENAS E IMEDIATAMENTE APÓS O ENCERRAMENTO DA LICITAÇÃO, tornando público apenas divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas.]

16. Justificativa técnica da escolha da solução

A aquisição da solução HSM garante a continuidade da capacidade de armazenar de forma segura as chaves criptográficas de todas as aplicações da SEFAZ que utilizam certificados digitais, evitando a diminuição do nível de segurança de rede e da informação das aplicações/serviços da SEFAZ

17. Justificativa econômica da escolha da solução

A aquisição da solução HSM garante maior nível de segurança às aplicações/serviços da SEFAZ evitando fraudes que possam acarretar prejuízos financeiros ao erário público.

18. Justificativa para não parcelamento

Tratando-se de aquisição de solução de Hardware Security Module – HSM, contemplando hardware, software, instalação /configuração /testes e documentação técnica, serviços continuados de suporte técnico, manutenção com reposição de hardware , atualização de software e treinamento, confluindo todos esses elementos para compor e operacionalizar um único sistema de HSM, não cabe o desmembramento do objeto em subitens de forma a permitir sua adjudicação a licitantes diversos. A contratação do objeto junto a um único fornecedor permitirá ademais a gestão integrada do atendimento técnico, remoto e local e ainda evita preocupações com divisão de responsabilidades que por si só já pode gerar problemas ou dificultar a resolução deles. Por esses motivos, os itens do item 7 da ETP deverão ser licitados pelo preço total do objeto, através do critério do menor preço global.

19. Justificativa para vigência plurianual

19.1. O serviço de suporte Técnico, manutenção com reposição de hardware e atualização de software para solução é enquadrado como serviço contínuo, sem regime de dedicação exclusiva de mão de obra, e sem predominância de mão de obra, sendo a vigência plurianual mais vantajosa, considerando os seguintes pontos :

Fundamentação Legal

19.1.1. A presente contratação em caráter plurianual encontra respaldo no artigo 107 da Lei nº 14.133/2021, que dispõe sobre a possibilidade de celebração de contratos com prazo superior a 12 (doze) meses, desde que relativos à prestação de serviços contínuos e que haja previsão no edital e vantajosidade para a Administração. O §4º do referido artigo reforça que a prorrogação sucessiva é permitida até o limite de 10 (dez) anos, desde que mantidas as condições de vantajosidade e interesse público

Continuidade de Serviço Essencial

19.1.2. O objeto contratual refere-se à prestação de serviço essencial e contínuo à Administração, cuja interrupção comprometeria significativamente o funcionamento das atividades institucionais. A contratação plurianual visa garantir a regularidade, qualidade e previsibilidade na execução do serviço, evitando descontinuidade que possa prejudicar o interesse público.

Ganhos de Economicidade e Eficiência

19.1.3. A adoção de contrato plurianual proporciona ganhos relevantes de economicidade e eficiência administrativa, ao reduzir custos operacionais relacionados à repetição de processos licitatórios, mobilização de equipes técnicas e transição contratual. Além disso, a possibilidade de negociação com fornecedores para prazos mais longos tende a resultar em condições comerciais mais vantajosas, refletindo diretamente na otimização dos recursos públicos.

Planejamento Orçamentário e Aderência às Normas

19.1.4. A contratação está devidamente alinhada ao planejamento orçamentário do órgão, com previsão de recursos nos instrumentos legais pertinentes, como o Plano Plurianual (PPA), a Lei de Diretrizes Orçamentárias

(LDO) e a Lei Orçamentária Anual (LOA). A autorização legislativa específica para a despesa está contemplada, conforme exigido pela legislação vigente, garantindo a legalidade e a responsabilidade fiscal da contratação. O prazo contratual superior a 12 meses atende à natureza contínua do serviço e está em conformidade com o art. 107 da Lei nº 14.133 /21, resguardando o equilíbrio econômico-financeiro do contrato.

Equilíbrio Econômico-Financeiro e Segurança Jurídica

19.1.5. O contrato será estruturado de forma a preservar o equilíbrio econômico-financeiro, com cláusulas que assegurem a revisão e reajuste de valores conforme índices oficiais e parâmetros legais. A Administração manterá a prerrogativa de extinguir o contrato, sem ônus, caso não se verifique mais a vantajosidade ou disponibilidade orçamentária, conforme previsto no §3º do art. 107 da Lei nº 14.133/2021.

20. Qualificação Técnica Operacional

O objeto de contratação visa garantir um alto nível de segurança no armazenamento de chaves criptográficas privadas, protegendo dados confidenciais e de aplicações críticas através do armazenamento e gerenciamento de suas chaves criptográficas com HSM bem como disponibilizar assinatura digital de alta performance, o que demanda um elevado nível de especialização da contratada para garantir : a integridade e confidencialidade de informações, o funcionamento contínuo da infraestrutura e a interoperabilidade com outros sistemas. A necessidade de comprovação de experiência compatível justifica-se pois: assegura que a contratada já executou soluções similares envolvendo HSM; reduz o risco de falhas na implantação e aumenta a probabilidade de cumprimento adequado dos prazos e níveis de serviço.

Ademais, a qualificação técnica visa também assegurar que empresa possua equipe especializada para implantar /testar/configurar e prestar serviços de suporte de forma a reduzir indisponibilidade da solução de HSM.

21. Contratação de Solução Híbrida

A contratação proposta visa atender aquisição de uma Solução de Hardware Security Module – HSM, contemplando hardware, software, instalação /configuração/testes e documentação técnica, serviços continuados de suporte técnico, manutenção com reposição de hardware, atualização de software e treinamento. A presente contratação é caracterizada como híbrida, pois contempla o fornecimento de bens: hardware e software e a prestação de serviços correlatos: (instalação/configuração/testes, suporte técnico, treinamento), de forma integrada e funcional.

A solução híbrida mostra-se mais adequada diante da interdependência técnica entre os componentes, garantindo desempenho e eficiência operacional à administração pública.

É constatado que há predominância do fornecimento de bens, tendo em vista maior representatividade financeira dos bens no valor total estimado e, portanto, os serviços têm caráter acessório /complementar.

22. Critérios de sustentabilidades

Seguem os critérios de sustentabilidades a serem seguidos:

I - os bens devem ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento; e

II - os bens não devem conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

23. Catálogo eletrônico de padronização

A não utilização do Catálogo Eletrônico de Padronização (ou Catálogo Eletrônico de Compras) no presente processo licitatório se justifica pelas características específicas do objeto definido no Termo de Referência nº 67 /2025, conforme exposto a seguir:

1. Natureza complexa e integrada da solução de TIC

O objeto da contratação consiste na aquisição de solução de Hardware Security Module (HSM), contemplando não apenas o fornecimento de bens, mas também software, serviços de instalação, configuração, testes, documentação, suporte técnico continuado, manutenção com reposição de hardware, atualização de software e treinamento. Trata-se, portanto, de uma solução integrada de tecnologia da informação, cuja execução depende da combinação de múltiplos elementos interdependentes, impossibilitando sua adequada representação por itens padronizados isolados disponíveis em catálogo.

2. Especificidades técnicas elevadas e requisitos de desempenho

A solução de HSM insere-se na categoria de equipamentos de segurança criptográfica, exigindo requisitos técnicos rigorosos, como interoperabilidade, confiabilidade, segurança da informação e desempenho operacional. Essas características não são plenamente contempladas em modelos padronizados do catálogo eletrônico, que normalmente abrangem bens ou serviços com especificações genéricas.

3. Predominância de solução sob medida e não padronizável

Embora o objeto tenha sido classificado como “bem comum” para fins licitatórios, sua composição demonstra tratar-se de uma solução dimensionada sob medida, ajustada às necessidades da infraestrutura e das aplicações da SEFAZ.

4. Necessidade de detalhamento técnico para garantir a adequada execução

A contratação envolve obrigações contratuais complexas, incluindo:

- serviços especializados de instalação e configuração;
- suporte técnico contínuo com níveis de serviço;
- manutenção com reposição de hardware;
- atualização de software;
- treinamento técnico de usuários.

Tais elementos demandam descrição minuciosa e controle por indicadores de desempenho (IMR), o que não é compatível com a estrutura simplificada do catálogo eletrônico.

5. Risco à eficiência e ao resultado da contratação

A eventual utilização do catálogo eletrônico poderia:

- restringir indevidamente as especificações técnicas necessárias;
- comprometer a aderência da solução às necessidades da Administração;
- gerar riscos à segurança da informação, dada a criticidade do objeto (HSM);

- resultar em contratação inadequada ou insuficiente.

Diante do exposto, conclui-se que a não utilização do Catálogo Eletrônico de Compras se justifica pela complexidade, especificidade técnica e natureza integrada da solução de TIC a ser contratada, a qual não encontra correspondência adequada em itens padronizados.

A adoção de descrição própria, detalhada no Termo de Referência, mostra-se medida necessária para assegurar a correta execução do objeto, a mitigação de riscos e o atendimento pleno às necessidades institucionais.

24. Benefícios a serem alcançados com a contratação

24.1 A aquisição de Solução de Hardware Security Module – HSM, permite que seja mantidas as seguintes funcionalidades: a) Proteção de dados confidenciais e de aplicações críticas através do armazenamento e gerenciamento de suas chaves criptográficas com Módulos de Segurança de Hardware; b) Armazenamento de chaves criptográficas em hardware inviolável e auditado.

24.2 A contratação do suporte técnico pretendida por essa contratação garante a atualização contínua da solução por parte do fabricante, incluindo correções (bugs) e melhorias do produto ao longo do ciclo de vida respectivo; e a cobertura do suporte dos equipamentos propicia a continuidade das proteções advindas da solução, o que beneficia e colabora para a manutenção de um ambiente seguro e estável para a infraestrutura de TIC.

25. Providências a serem Adotadas

Não há providências a serem tomadas.

26. Declaração de Viabilidade

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

26.1. Justificativa da Viabilidade

Esta Secretaria conclui pela contratação da solução especificada neste estudo técnico preliminar, considerando-se o valor estimado e o escopo definidos nesta ETP.

27. 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](#).

EDUARDO DO AMARAL

Auditor Fiscal da Receita Estadual



Assinou eletronicamente em 28/05/2026 às 10:11:55.

